Sector-wise Investigation of Bring Your Own Device (BYOD) Security Policies in Pakistan

By

Ayesha Sajid

00000317975

Supervisor

Dr. Yousra Javed

Department of Computer Science

School of Electrical Engineering and Computer Science (SEECS)

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

July 2021

Approval

It is certified that the contents and form of the thesis entitled "Sector-wise Investigation of Bring Your Own Device (BYOD) Security Policies" submitted by AYESHA SAJID have been found satisfactory for the requirement of the degree

Advisor : Dr. Yousra Javed

Signature: ____________

Date: 29-Jul-2021

Committee Member 1:Dr. Sana Qadir

Signature: Sana Qadir

Date: 29-Jul-2021

Committee Member 2:Dr. Mehdi Hussain

Signature: Hussain

Date: 29-Jul-2021

Committee Member 3:Dr. Dr Hasan Tahir

Signature: ____________

Date: 29-Jul-2021

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Sector-wise Investigation of Bring Your Own Device (BYOD) Security Policies" written by AYESHA SAJID, (Registration No 00000317975), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: ______________________

Name of Advisor: Dr. Yousra Javed

Date: 29-Jul-2021

Signature (HOD): ______________________

Date: ______________________

Signature (Dean/Principal): ______________________

Date: ______________________

Dedication

This thesis is dedicated to *my beloved parents*

Certificate of Originality

I hereby declare that this submission titled "Sector-wise Investigation of Bring Your Own Device (BYOD) Security Policies" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: AYESHA SAJID

Student Signature: ______________

Acknowledgments

First of all, I would like to thank my Almighty Allah for making me capable of achieving all this. Then I would like to thank my parents for their continuous support and guidance. Here, I would especially like to mention the efforts of my father who used to drop me to my university, wait there in the parking till my classes would end, and then take me back home just to ensure my comfort and so that I do not have to go through the hassle of availing the university transport.

I want to thank all of those family members, friends, and old teachers who have especially prayed for my success and also helped me in the best of their capacities. One special person that I can certainly not forget. My partner. I want to thank him with all my heart for all of his lovely prayers, wishes, and support without which I would definitely not be able to stand where I am today. Then, I want to extend my gratitude towards my thesis supervisor **Dr. Yousra Javed** who took the responsibility of guiding me throughout this journey.

Last but not the least, I want to thank all of my honorable GEC members **Dr. Mehdi Hussain**, **Dr. Sana Qadir**, and **Dr. Hasan Tahir**. Their valuable feedback motivated me to put in all my efforts into making this thesis a noteworthy research contribution. In the end, I just want to say that achieving this degree was a collective effort of so many people and I, alone would never be able to do this on my own. Another thing that I have learnt through this journey is that no matter how difficult situation you are in at the moment, if you are persistent and sincere with your efforts, there is nothing in this world that you cannot achieve obviously by the will of Allah Almighty.

Contents

List of Abbreviations and Symbols

Abbreviations

BYOD	Bring Your Own Device
SQ	Survey Question
RQ	Research Question
MDM	Mobile Device Management
TPA	Third Party Applications
NAC	Network Access Control
MAM	Mobile Application Management
SME	Small and Medium Enterprise
2FA	Two Factor Authentication
API	Application Programming Interface
PPT	People Policy Technology
VPN	Virtual Private Network
PHI	Personal Health Information
LAN	Local Area Network
WLAN	Wireless Local Area Network

RBAC	Role Based Access Control
MIM	Mobile Information Management

List of Tables

List of Figures

Abstract

With the advancement in technology and pervasiveness of computing devices, new practices have been adopted by various organizations to optimize their infrastructure and to efficiently utilize the available resources and increase productivity while consuming lesser resources. One such effort was the introduction of Bring Your Own Device (BYOD) concept, to let the employees bring their personal devices to the workplace for the tasks assigned to them.

Prior to the introduction of Bring Your Own Device (BYOD), companies used to provide their own resources to the employees, and those resources were managed centrally by the organizations. However, as soon as the organizations shifted to the BYOD approach, they lost control over those resources, and were unable to employ their best security practices to the devices that are not owned by them. Therefore, the BYOD approach has left us with numerous security concerns. For instance, suppose that an employee is not in the premises of the organization and he tries to share a critical file with his colleague via an insecure free Wi-Fi available in a coffee shop. Doing this will provide a golden opportunity to a hacker to break into the employee's personal device and hence steal the critical data.

The goal of this thesis is to investigate BYOD in four sectors, namely, **Information Technology** (because almost 75% of the cyber security attacks are targeted towards the IT industry), **Banks** (because they provide monetary benefits to the intruder if he successfully manages to break into their systems), **Military** (because their data is highly critical and is enough to destroy a whole country if it is misused by an enemy), and **Hospitals** (because the patients' information is very sensitive and can prove to be fatal for a patient if is illegally modified). More specifically, the following aspects will be investigated for each sector:

- What was the organization's experience as they shifted from the traditional desktop based approach to the BYOD approach
- What security issues they encountered with the BYOD approach and how did they tackle them
- What differences between the two approaches are responsible for these security issues
- Which security issues still remain unattended

The findings from this study will help assess the current state of BYOD policies and their implementation in various sectors of Pakistan, along with the similarities and differences in BYOD policies between the different sectors in Pakistan. This information will be used to propose a BYOD security framework and to give recommendations to the four selected sectors with which we can ensure best possible security even while complying with the BYOD approach.

Keywords: *BYOD, BYOD Policies, Security Issues*

Chapter 1

Introduction

1.1 Background of the Bring Your Own Device (BYOD) Approach

Every organization today strives very hard to optimize its infrastructure and efficiently utilize the available resources. It intends to increase productivity while consuming lesser resources. To achieve this goal, an important step was the introduction of Bring Your Own Device (BYOD) concept. This concept was intended to let the employees bring their personal devices to the workplace for the tasks assigned to them. This policy has recently been adopted by most of the organizations belonging to different industrial sectors, however, it comes with many security concerns as the organizations cannot employ their best security practices to the devices that are not owned by them.

For ensuring security while complying with the BYOD concept, most of the organizations came up with this idea of designing dedicated BYOD Privacy and Security Policies. Today, some organizations have dedicated BYOD Privacy and Security Policies in place while others have incorporated specific clauses related to BYOD in their General Privacy and Security Policy. Unfortunately, there are still some organizations who have allowed this practice without employing a proper policy. Moreover, another important thing is that a BYOD policy is always as good as an organization's ability to implement it. Therefore, solely relying on a BYOD policy for ensuring an organization's data security was not advisable. Nevertheless, we can still not completely disregard the importance of a good BYOD policy and the features that make it strong enough for ensuring security.

1.1.1 Importance and Features of a BYOD Policy

A policy refers to the set of guidelines and principles laid down by an organization to define the acceptable behaviour within the organizational premises. If we talk about a BYOD policy in particular, then such a policy will contain all those rules and regulations that are to be followed while allowing this practice at the workplace. These rules and regulations are there to ensure both the privacy and security of the organization and its employees while they are bringing and using their personal devices at the workplace. This is exactly why we cannot overlook the significance of having a BYOD policy in place.

However, there are some important features that must be present in a good BYOD policy for serving the intended purpose. These features are listed below:

- Clearly state (who) is allowed to use his personal device and in (which) situation.
- Ownership of the device should be clearly stated.
- Should include a clear statement about the requirements of security and compliance.
- Should clearly state which device features will be accessed by the organization.
- Clearly describe the details about data ownership.

1.1.2 Level of Research already Carried out in this Domain

The emergence of the concept of BYOD dates back to 2005 but this concept gained popularity in 2009. At that time, only the benefits of adopting this approach were perceived by the users, however, gradually the people also started realizing the drawbacks associated with it as it can also lead to some very serious privacy and security issues. Nevertheless, this realization did not give rise to any noteworthy contributions in this domain.

The only solution that most of the organizations came up with was to abandon this approach altogether to ensure privacy and security. The organizations that still hold onto this approach considered creating more strict BYOD policies, however, the compliance of these policies was still an issue. In this regard, a thorough research was needed which is not only capable of exploring the human factors associated with BYOD security but can also ensure best possible security while complying with this approach.

Therefore, the research in this domain up till now is very little. Most of the researchers have managed to highlight almost all the major concerns with the BYOD approach but they still could not devise a strong BYOD security framework or a set of good recommendations to tackle these concerns, except for creating a strong BYOD policy.

1.2 Motivation of doing Research in the Selected Domain

Since today we live in a world in which data breaches occur almost every other day, therefore, ensuring our privacy and security has never been this important ever before. Moreover, the research in our selected domain is very little all across the world but the research carried out in Pakistan in particular fails to address this issue.

Also, the four sectors that we have selected for our research namely, Banks, IT Industry, Military, and Hospitals are considered as hot-spots of privacy and security breaches. The reason behind this is the criticality of the data that these sectors deal with. That is why it always attracts the attention of the intruders because of which it becomes a necessity to explore the BYOD issues particularly in these four sectors in Pakistan.

1.2.1 Examples of a BYOD Security Risk

Consider an employee who has the access to his organization's crucial data through his personal device. Now since this device is not owned by that particular organization, therefore, it is quite possible that it might not comply with the same security standards set up by the organization for its own devices. Giving the access of the corporate data to such devices can pose a very serious risk to it and may even lead to its compromise.

Now consider another example scenario in which an employee has the liberty to access or even modify the corporate data through his personal device. An employee is not bound to work with the same organization forever, therefore, he might leave the organization at any moment. In this situation, if the proper access revocation processes are not performed once the employees leave an organization, then your data is always at the risk of a breach. Same is the case with a lost or a stolen device.

1.2.2 BYOD as a Challenge

Despite all the benefits of using the BYOD approach in different organizations, can the implementation of this approach still be challenging for us? This question emerges in the minds of most of the technical staff of the organizations. The answer to this question is a "YES". We all understand how the usage of personal devices at the workplace can prove to be cost-effective. However, when it comes to actually using the personal devices at the workplace, then there are certain measures that are needed to be taken before that.

By now, we totally understand that the usage of personal devices at the workplace can left us with lots of different vulnerabilities. Therefore, we must take some precautions to avoid any unwanted incidents. The most common precautionary measure out of these is the deployment of a mobile device management (MDM) software. The deployment of this kind of a software is always very demanding and as far as its cost is concerned, then you again need to spend a handsome amount of money on it to make it work properly. In this sense, we can say that the actual implementation of the BYOD approach within an organization can be very challenging.

1.3 Problem Statement

The lack of research regarding the security implications of using personal devices at workplace in the four sectors namely: **IT Organizations**, **Banks**, **Military**, and **Hospitals** in Pakistan.

1.3.1 Objectives of the Selected Research

The expected objectives of our research are listed below:

- To explore the experience of the organizations when they shifted from the traditional desktop based approach to the BYOD approach.
- To figure out the issues encountered by these organizations and the measures that they took to deal with them.
- To get the opinions of the representatives of these organizations on the probable causes of these security issues (including both the human and technical fallacies).
- To pinpoint the issues that still remain unattended.
- To propose a BYOD security framework that can easily fit into the environment of our four selected sectors.
- To give recommendations to deal with these issues effectively without the need of saying “NO” to the BYOD approach.

1.3.2 Research Questions

We have formulated the following high-level research questions for our study:

- **RQ-1:** What are the main differences between the traditional desktop-based approach and the BYOD approach according to the participants of the four selected sectors?
- **RQ-2:** What are the issues that arise as a result of shifting from the traditional approach to the BYOD approach?
- **RQ-3:** How are the organizations from the selected sectors tackling with these issues?
- **RQ-4:** What are the BYOD security issues that still remain unattended within these organizations?

1.4 Proposed Solution

Firstly, we want to conduct a survey across all the four selected sectors (with both the employees and the senior management) in Pakistan to find out the differences between the traditional desktop based approach and the BYOD approach. Through the responses of that survey, we wish to list down all the issues that were being faced because of shifting to the BYOD approach and the solutions devised by the respective organizations in Pakistan. By these responses, we also intend to investigate the root cause of the security issues with the BYOD approach.

Finally, with the analysis of the survey responses, we want to make ourselves able to propose a BYOD security framework and also a set of recommendations to ensure best possible security even while using the BYOD approach within our four selected sectors based on the observations of the above research. Moreover, we will also be able to investigate the current status of the BYOD policies and their compliance within different organizations belonging to the different sectors of Pakistan.

1.4.1 Relevance of this Research to the National Needs

The value and importance of the data within the Military and the Healthcare Industry can easily be perceived by everyone out there. Therefore, we cannot afford to compromise our security within these sectors because of complying with the BYOD approach even in Pakistan. However, as far as the Financial sector is concerned, then in the year **2018**, the data of almost all the banks within Pakistan got hacked which is why this topic holds a very crucial value within the Financial Industry of Pakistan. Lastly, almost **75%** of the cyber security attacks are directed towards the IT Industry. Therefore, we must not neglect the implications of using personal devices in the IT sector of Pakistan.

1.4.2 Expected Advantages of this Research

The expected advantages of this research are stated below:

- Increased awareness within the employees of various organizations about the effective usage of the BYOD approach without compromising their security. Moreover, the survey for this research is designed in such a way that the participants will be able to realize the importance of BYOD security even while filling in the survey.

- Increased productivity and lesser infrastructure expenditure. This can be done once the employees will be using their personal devices at the workplace while complying with the BYOD privacy and security policies of their respective organizations. This will not only reduce the infrastructure cost but will also enhance the productivity of the employees since they are naturally more comfortable while working with their personally owned devices.

- A significant decrease in the security and privacy issues due to the misuse (both deliberate and unintentional) of the personal devices at the workplace. This will happen because this research aims at educating the employees of various organizations belonging to the different sectors of Pakistan about the correct usage of the personal devices at the workplace without comprising the data that is either residing in those devices or the data to which these devices have access.

Chapter 2

Literature Review

2.1 General State of BYOD till Date

With the advent of BYOD, the businesses started enjoying all the perks of having employees that bring in their personal devices to the workplace. This meant that the organizations managed to save a major expense that was earlier spent on the infrastructure. Along with that, they also managed to see their employees working with their full potential and hence they became all the more productive. However, on the other hand, this paradigm also gave way to many new security challenges to those organizations of the business world who have openly embraced the BYOD approach.

To throw light on the major BYOD security issues and their devised solutions, [1] was a research conducted in 2015. The main motive of this research was to explore the top most challenges that emerged as a result of BYOD adoption and the countermeasures that were adopted to tackle with these challenges. A general observation that has been shared in this research is that since the time BYOD has come into play, the security attacks are mainly targetted to the mobile devices and most of these attacks are software-based.

The security challenges that were highlighted in this research were divided into four different categories namely: Challenges with the Deployment, Challenges with Technology, Challenges with Policies and Regulations, and Challenges with the Human Aspects or Psychology. As a part of these four categories of security challenges, access control or access rights permissions was at the top of the list. When the employees have access to shared data through their personally owned devices, they are more likely to make careless modifications.

Although, the mobile device management (MDM) tools are readily available in the market for gracefully managing the personal devices at workplace, however, these tools also have certain limitations. The top most limitation of such tools is that they can only support a finite number of devices but we all know that technology is progressing at a very fast pace because of which we cannot expect all of our employees to use the same kind of personal devices. It means that their personally owned devices will differ from each other in make and model because of which it is extremely challenging for an MDM software to manage all those devices.

While deploying BYOD security solutions, they are not as simple as they seem to be. You need dedication and commitment in terms of both time and money for these solutions to work as intended. Another aspect of the BYOD security issues is that once an employee is having corporate data on his personally owned device, then it gets very difficult for the organization to monitor it continuously. Hence, it becomes extremely challenging to prevent that data from being leaked, lost, stolen, or modified.

Also, when the employees connect their personal devices (containing corporate data) to insecure freely available Wi-Fi networks, then this can prove to be a fatal threat for that device as well as the data residing on it. It is so, because that insecure network might prove to be a source of installing malware on the device hence corrupting the data residing on it or rendering the device useless for a whole lifetime. Moreover, when the corporate data resides on an employee's device, the employees are mostly free to save it on the Cloud. Afterwards, even if they do delete that data from there, it is never completely purged since the Cloud also maintains a regular backup of that data.

The development of a strong BYOD security policy is also very challenging especially for those organizations that operate globally. It is so because such organizations have to devise their policies in such a way that they perfectly align with the rules and regulations set up by all those regions in which that organization is operating. It should also be taken into consideration that the security solutions employed to protect the organization's security should not prove to be invasive to the employees' privacy.

Lastly, the employees should be provided with proper training in regards to the correct usage of the BYOD approach. Moreover, this should not be a one time practice since humans tend to forget things over the time. Therefore, periodic training sessions are mandatory. This fact should also be taken into account that the employees who are generally against the restrictions imposed on them by the organization's BYOD security policy have a very high tendency to find workarounds and hence, they are highly likely to break the rules consequently comprising the corporate data.

Talking about the security frameworks discussed in this paper, the research under discussion categorized these frameworks into two distinct categories i.e. General Purpose BYOD Security Solutions and Single Purpose BYOD Security Solutions. The former category included frameworks such as network access control (NAC), mobile application management (MAM), mobile device management (MDM), etc. whereas the latter category included solutions such as containerization, anti-virus, remote wiping of data, etc. Regardless of the purposes for which they are used, all of these security frameworks had their own pros and cons.

This research concluded with a discussion on the limitations of some of the existing security frameworks. MDM tools are not welcomed by the employees of the organizations since they feel like such tools are imposing unnecessary restrictions on them. Generally, the network security solutions that are available in the market are very expensive and also, they do not offer any protection against data leakage. Finally, the remote wiping of data is only helpful until your data is not actually compromised. Once it has already been used for serving any illegal purposes, then employing this solution afterwards is absolutely useless.

Some researchers are also of the view that the organizations also need to consider the perspective of cyber-security threat while employing BYOD. [2] was a research conducted in this regard. It highlighted that as compared to larger organizations, small and medium enterprises (SMEs) are more prone to cyber-security threats. It is so because the larger enterprises have a better understanding of these concepts whereas SMEs have restricted resources because of which they cannot spend much on their security infrastructure. This is exactly why SMEs are an easy target for the cyber-security hackers.

Along with broadening their perspectives on the understanding of cyber-security threats, SMEs should also focus on the teaching and training of their employees regarding BYOD adoption while incorporating a sound security framework. Here, we should also not neglect this fact that the applications that are installed and used on the personal devices at workplace might come from unlicensed sources which means that they can also prove to be potentially harmful for corporate data. Furthermore, the security policy creation is one thing but we must also not forget to properly communicate these policies to all the employees of the organization so that all of them are well-aware of their responsibilities.

Apart from that, another realization to be made over here by the SMEs is that they should know that the cost spent on security solutions is far less than the cost spent on the recovery of compromised data. Therefore, they must not take this thing for granted. Lastly, IT security auditing is also very important. With the help of this security assessment and analysis, all the loopholes of the existing security frameworks can be figured out and fixed. Also, we can easily get to the root-causes of all the security issues by looking at these audit reports.

While adopting BYOD, we must not forget about the privacy and security risks that are associated with the paradigm of BYOD. BYOD had also started leaving an impression on to the educational institutions of Malaysia. To explore this further, [3] was a research conducted with the educational institutions of Malaysia. This research explained that most of the educational institutions of Malaysia have adopted BYOD while also incorporating some form of network access control (NAC). However, the absence of a sound BYOD security policy in such institutions exposed them to very severe security vulnerabilities.

The goal of this study was to understand the perceptions of today's modern generation regarding BYOD and the security challenges that are associated with it. In this regard, a survey was conducted with 60 students of a Malaysian university out of which 39 were males and 21 were females. This survey contained Likert Scale type questions. In a nutshell, the main finding of this survey was that most of the respondents were not familiar with the procedures of enabling security controls such as 2FA, pin codes, passwords, on their BYOD devices. Because of this, it is mandatory for the educational institutions to work on the proper training of the participants before allowing them to use personal devices within the educational institutions.

Stepping a little further, [4] was a research carried out to investigate how information security and privacy can be ensured within the environments that have already embraced the BYOD paradigm. The main focus of this paper was on the risks associated with BYOD and their respective mitigation strategies. We all understand that a properly implemented BYOD policy can result in the benefits of both the employees as well as the organization. The employees can become more productive as a result of using their personally owned devices whereas the organizations can save their money spent on these IT resources.

Although, it is very easy to highlight the BYOD security issues, however, it gets very difficult for the management of an organization to understand which security issue should be most focused on for ensuring a safe and secure BYOD environment. To investigate this problem, this research formulated a set of different research questions. We can integrate all these research questions into one by asking how both privacy and security can be ensured simultaneously while complying with the BYOD approach.

This study used a qualitative research approach by conducting interviews and distributing questionnaires among the research participants. The target participants numbered 62 and they belonged to three different organizations. To analyse the collected data, the thematic analysis approach was adopted with the intention of deriving themes from the collected responses and then devising a description of all of those themes. To ease this process a little further, NVivo software and SPSS were used for identifying themes and analyzing them efficiently.

This study revealed some very interesting findings. Some target organizations have still not designed sound BYOD security policies because of which there is a dysfunction in the whole organization. Along with that, some organizations do have BYOD security policies in place but there is still a question mark on their enforcement. Also, there are some senior employees who are absolved from complying with these policies because of which there exist a large number of security loopholes within the organization.

Moreover, there are certain organizations who have forbidden the usage of some particular type of personal devices at the workplace considering in mind their security vulnerabilities. Nevertheless, some employees were still using those forbidden devices within those organizations without even bringing it in the knowledge of the senior authorities. Another aspect of BYOD security issues was that when a problem did arise, some employees were even unaware of the next step they should take in this regard to secure their precious data.

All the participants involved in this research were of the view that BYOD adoption can prove to be very productive since it positively impacted the performance of individual employees as well as the whole organization. This research suggested a layered approach for the implementation of a BYOD policy. These layers should be mainly comprised of BYOD and BYOD security controls implementation, properly conveying the policies to the concerned employees, risk control and maintenance of the already existing policies. The only limitation of this research was that it did not contain any quantitative data and also, that the sample size for this study was relatively smaller.

While conducting a research on the security issues, it is always good to draw a comparison between the security cultures of two different environments. To address this, [5] was a research carried out with 128 and 118 participants of USA and Italy respectively. This research pointed out that the main idea of the organizations behind adopting the BYOD approach was that their employees do not necessarily need to be at their desks for work all the time rather they can work from anywhere and at any time they want.

The survey for this study was divided into two parts. The first part contained all the demographics questions whereas the second part contained the Likert Scale type questions regarding BYOD security policies within the respective organizations of the selected participants. The collected data for this research was analyzed using the Univariate ANOVA Test. The findings of this study revealed that the participants from USA and Italy both did not give due importance to BYOD security policies and the data protection of their devices. Finally, this study suggested that the security education training and awareness (SETA) programs must be carried out periodically within the organizations wishing to adopt BYOD.

For fighting with the issues that emerged as a result of BYOD adoption, numerous efforts were put into place. [6] was an effort in this direction to devise a deep learning framework for combating the security risks arising as a result of BYOD adoption. A survey carried out earlier in USA revealed that almost 95% of the employees of various organizations were habitual of using one or other type of personal devices at their respective workplaces. The reason behind the inclusion of artificial intelligence in this whole scenario was that the researchers wanted to make the MDM solutions all the more robust so that they can easily adapt to the changing policies and procedures of the organizations.

The main goal of this research was to formulate a mechanism using artificial neural networks and decision tree machine learning to detect all the unauthorised access attempts and this mechanism should be powerful enough that it can minimize the impact of such invasions. This mechanism or framework will base its decisions on the current context and in this way, the decisions made by such a model will be more accurate. This context will be created while looking at the five Ws i.e. What? Where? When? Why? and Who? Hence the information derived by looking at these contexts will be highly comprehensive to take the best possible security decision.

This research also provided the equations for calculating the true positives, true negatives, false positives, and false negatives of the proposed model. Two different experiments were then carried out to test the effectiveness of the proposed model. In short, the model under discussion worked in two different phases i.e. detection of the dynamic context and taking the appropriate decision using machine learning. The overall precision and accuracy of this model found out as a result of the experiments that were carried out was more than 99% which depicts a very high success rate of the proposed model.

[7] was a research carried to propose a BYOD specific risk management framework. According to the researchers, most of current risk management solutions focus on network security which is why they cannot be adopted as it is for the BYOD approach where every employee is using his/her personal devices at the workplace. The framework that has been proposed in this research worked by looking at the MDM log file to trace out all the security breach events and their probable causes.

The MDM log files do not only help us with network device failures but they can also help in tracing the lost or stolen devices through their locations. In this way, these log files enable us to perform risk management in real time. Once these log files are carefully analyzed, the data from them is labelled and classified so that it can be used for the training and testing of the proposed model. The experimental results showed that the accuracy of the proposed solution was 99% which meant that this research has proved to be a noteworthy contribution in the field of BYOD security.

The acceptance or rejection of any new technology depends largely on the perceived value of that technology by its target audience. To understand this, [8] was a study conducted in USA in 2019 to realize the perceptions of employees on IT consumerization. This research highlighted that BYOD was welcomed the most by such employees who were supposed to have frequent interactions with the clients. In addition to this, the research on BYOD before this study mainly focused on an organizational perspective whereas the perspective of employees was totally neglected.

This study shared that allowing personal devices at workplace can help greatly in increasing the employees' productivity. Moreover, the employees who were allowed to bring their personal devices to the workplace were more satisfied with their jobs. However, a major drawback of using personal devices for work was that the distinction between personal and professional life got blurred as a result of which there was a disturbance in the work-life balance of the employees.

This research is based on the Prospect Theory according to which people always make decisions according to the perceived value of the subject under discussion. This perceived value is a combination of the benefits obtained and the losses incurred. This research was based on both the qualitative and quantitative data analysis methods. The researchers developed a few hypothesis before conducting this study and tried to validate them through the results derived. Three out of the seven formulated hypothesis held true according to the research that was carried out.

According to the supported hypothesis, job flexibility, empowerment of technology usage, and enjoyment led to the adoption of the BYOD approach. However, this research also had some shortcomings. First of all, this research was based on the self-reported data because of which the results lacked reliability. Secondly, the participants of this study were selected only from USA because of which its results cannot be mapped on to other countries without making necessary modifications.

Even after developing strong BYOD policies, their compliance was still an issue for most of the organizations out there. To address this concern, [9] was a research carried out in USA to highlight the employees' intentions while complying with the BYOD security policies. This paper opens up with a discussion on the most common implications of using personal devices at workplace. A clearcut remark given at the very begining of this research was that to ensure the correct BYOD usage and for achieving the benefits of this approach to the fullest, both technical and non-technical measures should go hand in hand.

This research was mainly based on the Protection Motivation Theory (PMT) and by making use of this theory, the researchers intended to highlight all those key factors and features of BYOD that cause a hindrance in the employees' compliance of the BYOD security policies. This research strongly suggested that all the BYOD security frameworks must be based on the PPT model. Moreover, the researchers were also of the view that the future BYOD security frameworks must integrate MDM along with next generation firewalls. Apart from that, due consideration should be given to the application programming interface (API) level security solutions since they are way more cost-effective.

This research was carried out solely to fill in the gaps found in the literature such as conducting research with the organizational employees instead of the university students who were not even exposed to the proper usage of personal devices. The main hypothesis formulated before conducting this research was that the employees are more likely to comply with the BYOD security policies when they perceive the threats to be real and feel the likelihood of the occurrence of those threats to be higher. Similarly, when the employees will perceive the risks to be lower, they will consequently start behaving more carelessly.

Also, when the employees perceive the cost spent on a security solution to be higher than its benefits, then they are less likely to go in favour of that security solution. This research was carried out while conducting online surveys with the employees of those organizations who were already practicing the BYOD approach. This survey was comprised of Likert Scale type questions to figure out the employees' threat appraisal and coping appraisal. The threat appraisal corresponded to the employees' perception of the severity of the security threats whereas the coping appraisal referred to how the employees responded when they faced a security threat.

The proposed research was assessed while using the techniques of partial least square approximation. The findings of this research showed mixed results i.e. some of the hypothesis of this research were supported while others were not. This research suggested that even after developing BYOD security policies, the organizations should direct their efforts on how well these policies are complied with. For that, they need to continuously monitor the employees' behaviour at least within the organizational premises. As far as the limitations of this study are concerned, then the target audience of this study mainly belonged to USA because of which its results cannot be generalized. Secondly, the study only focused on two factors of BYOD that can have an impact on the employees' intentions of complying with BYOD security policies.

Whenever we intend to train our employees for any new technology, it is mandatory to design that training in such a way that it goes in favour of that technology. Similarly, the BYOD security policies and training should also be developed in a way that they persuade the employees to opt-in for using their personal devices at the workplace immediately. To throw light on this, [10] was a research conducted in China in 2019. The aim of this study was to explore all those factors that affect the employees' decision of complying with BYOD security policies.

To do so, a survey was conducted with some of those organizations of China that have allowed the BYOD practice for their employees. Some hypothesis were formulated prior to conducting this study and they were tested using an experimental survey with the said organizations of China. In this survey, the participants were mainly asked about their views on developing a BYOD security policy. In addition to that, their knowledge regarding the implementation and working of the BYOD approach was also tested with various questions. A total of 175 participants from these organizations took part in this survey.

To analyse the results of this study, ANOVA and T-test were used. The main finding of this study was that the BYOD security policies should be developed and conveyed to the employees before the actual implementation of this approach within the organization. Doing this will positively impact the usage of personal devices at workplace as it will clear all the misunderstandings beforehand. Secondly, the BYOD security policies should be conveyed to the employees in such a positive manner that they not only embrace this practice readily but also comply with the BYOD security policies religiously. However, more emphasize should be payed in the future on the scenarios in which an employee has the liberty to change his decision once he has opted to adopt the BYOD approach.

Whenever a security issue arises in an organization, the work practices of its employees change in a way that they are best suited to the current situation and they should be such that they are able to minimize the effects of the damage that has already been done. Similarly, when the employees find their data to be vulnerable because of following the BYOD practice, they naturally tend to get more hesitant as a result of which their further continuity to work with their personal devices gets questionable and doubtful. To address this issue, [11] was a very recent study conducted in 2020 in China to figure out whether employees continue to work with their personal devices or not in case of an information security related conflict.

For that, a survey was conducted with 235 employees from the IT and Finance sectors of China. First of all, a series of hypothesis were formulated in this regard. If we integrate them all into one, then we can say that, an information security issue always gives rise to information security fatigue as a result of which the employees' adoption of BYOD gets negatively affected. To analyze the data collected from this survey and for validating the formulated hypothesis, quantitative data analysis and structural equation modelling were used. The success of this study can be realized from the survey results that rendered the formulated hypothesis to be true.

This study suggested that in order to avoid information security fatigue, organizations should direct their efforts on conflict management and emotional management of their employees. A sound conflict management can be done by doing practices like regularly upgrading their security policies in a way that they are right in accordance with the current security standards. On the other hand, emotional management can be done by encouraging the employees to take part in BYOD security policy making in order to understand their perspectives regarding BYOD adoption in a better way. Although this study was a great step forward in this direction, however, the only limitation of this study was that it focused only on the IT and Finance industries of China. Therefore, it has been suggested in this research to direct future studies to focus on other industrial sectors as well to get a broader picture of BYOD adoption.

Uptil now, we have talked about the different issues that can arise as a result of BYOD adoption, however, we still have not specifically looked at the legal issues which BYOD adoption can give rise to. To explore all such legal issues and their possible mitigation strategies, [12] was a research carried out in 2016. This research aimed to highlight the current state of BYOD along with some future predictions regarding its adoption. It discussed various legal issues that can be caused as a result of using personal devices at the work place. Finally, this study gave some recommendations regarding the proper BYOD usage to avoid all those legal issues in the best possible manner.

Some very interesting statistics were highlighted at the beginning of this paper. According to the researchers, almost 85% of the organizations give the liberty to their employees to bring in their personal devices to the workplace whereas only 30% of them have proper BYOD security policies in place. This can lead to some major security issues that will have to be dealt with later on. Furthermore, less than 50% of the organizations take the responsibility of securing the devices used for the BYOD program whereas the rest of them rely on the employees for securing their devices and the data residing on them. Moreover, almost 53% of the BYOD users install third party unsupported apps on their devices that they use for work related purposes.

Keeping in mind all of these statistics, this research mentioned some of the very critical legal issues that arise due to the carelessness in employing the BYOD practice. Data maintenance and storage became a very serious concern when personal devices were used for accomplishing official tasks. When the corporate data became available on public networks or the employees were allowed to even store it in their personal devices, then this caused a major threat to the integrity and confidentiality of that data. Secondly, it was very difficult for the organizations to implement their best security practices on the employee-owned devices which caused another security loophole.

Another legal issue was that the personal devices that were being used at the workplace also contained private data of the employees. Therefore, employing a security control for the corporate data on such devices might also mean breaching the employees' privacy. Yet another aspect of such issues was that some of the employees were unaware of the next step they should take in the event of a security disaster. Moreover, in the case of a data breach, the organization might want to wipe out all the data residing on the employee's personal devices hence leading to the loss of the employee's personal data as well. Lastly, the employees had the liberty to change their personal devices whenever they wanted. In that scenario, the secure destruction of the corporate data residing on such a device was also a very challenging task to deal with.

Finally, this paper suggested some potential mitigation strategies for all of these legal issues. First of all, clear-cut BYOD security policies should be formulated and they should be effectively conveyed to all the concerned employees. Data profiling and containerization should be actively used. Mobile devices should be secured with the best possible security solutions and VPNs should be used for communication over the network. Proper incident response plans should be put into place. Moreover, employing a corporate data security solution must not breach the employees' privacy. Therefore, the security solutions must be designed in such a way that they prove to be beneficial for both the organizations and their employees.

Some of the organizations do not have proper BYOD security policies in place because of which they are generally hesitant to adopt this approach. In this way, they deprive themselves of the numerous benefits that this approach offers. Therefore, there should be some national level policy making guidelines for all such organizations. To cater to this problem, [13] was a study formulated in Ecuador to highlight some of the national cyber-security policy making guidelines. This paper also began with the brief introduction of all those BYOD security issues that the organizations who are practicing this approach were currently facing.

This paper gave some recommendations for the organizations aiming to devise BYOD security policies. First, it should be strongly advised to the employees to keep their personal devices password-protected. These passwords should be strong enough to combat any password cracking attacks. Employees should be provided with all the white-listed apps that they are allowed to install on the devices that they are using for the office work. They should be encouraged to immediately report to the concerned authorities in case of a lost or stolen device. Moreover, the employees should also be restricted to share their BYOD devices with any third person to avoid data leakage.

Employees should also not be allowed to store the corporate data on their personal devices rather they should be enabled to access it via a shared storage that is owned by the organization so that its security can be ensured. They should use an appropriate security software that is perfectly compatible with the personal device that they are using at the workplace. The control and monitoring of the personal devices at the workplaces should be centralized so that it gets easier to catch all the potential bugs. Finally, this paper suggested the usage of private clouds for storing data for providing an added layer of security.

Industry 4.0 or the Fourth Industrial Revolution refers to the usage of the latest technology such as smart devices for automation of the commonly occurring tasks. The BYOD concept is also a product of this industry 4.0 paradigm and to sum up the challenges that emerged as a result of this industrial revolution, [14] was a research conducted in 2017. The first step towards mitigation of an issue is its realization. According to this research, there is no doubt about the exceptional benefits that this revolution has brought about, however, on the same side, it has also given rise to many new security challenges.

The BYOD concept was also called as Bring Your Own Daemons in this paper because of all the security issues that it gave rise to. As a result of the added ease provided by this approach, the corporate data got highly vulnerable because of which the organizations practicing this approach were in a dire need of efficient security solutions. The most critical BYOD security issue highlighted in this research was data confidentiality breach which occurs as a result of providing escalated privileges to employee-owned devices. When the employees will be allowed to access corporate data with their personal devices without employing proper security controls, these daemons will continue to threat the confidentiality of the corporate data.

The very first step towards the exposure of your critical data starts with an unauthorized person getting the privileges to access it. It means that while addressing all the security issues, we must not over look the importance of proper access control mechanisms. To link up the network access control phenomenon with the BYOD concept, [15] was yet another research carried out in 2017. This research work aimed to create an intelligent filtering technique for gracefully managing the network access control with BYOD using artificial intelligence.

The model proposed in this research worked in two different steps. Firstly, the device behavior profiling was done for enabling the model to intelligently filter the data packets. Once this component was built, the next step was to use this component for applying filtering techniques for detecting all the potential anomalies in the devices' behavior. For the proper classification of the behavioral data, K-Means clustering was used. Finally, the performance of the proposed model in this research was experimentally evaluated which was fortunately very accurate.

[16] was another attempt in the BYOD access control domain which was in fact an improvement in the model proposed in the research discussed above. In this new model, the step-wise access control procedures were defined for a new user and a returning user. According to this model, whenever a new user will try to access an organizational network, the request will first pass through the access control component from which it will be passed on to the adaptive intelligent filter. This filter will extract the device's features and perform the user profiling. This user profiling will formulate the normal behaviour of that user, store it, and then register that user as a legitimate one.

After doing this, whenever a request will be received at the access control component, instead of passing it directly on to the adaptive intelligent filter, it will first be directed to the user authentication module. If the user is authenticated, only then the request will be transferred to the adaptive intelligent filter from where all the abnormal behaviors (if any) will be detected. If the request is found to be legitimate and trustworthy over here, only then a successful login will take place. Otherwise, the login attempt will fail while rendering an error message.

Up till now, we have been talking about the BYOD security issues and their mitigation strategies. However, we did not pay much attention on to the assessment of the overall

BYOD infrastructure. [17] was a research conducted in this domain in 2019. In this research, a security assessment model was proposed to analyze the current BYOD security status within an organization. Moreover, this model was tested by applying it for the assessment of the BYOD security posture of a hypothetical organization.

The model proposed in this research work suggested a modular as well as a holistic approach for assessing the overall BYOD security posture of an organization. According to the proposed model, four different security components namely: Management Security, User Security, IT Security, and Mobile Device Security must work together to ensure a well-secured BYOD environment. Once the security of these individual components of an organization will be ensured using the proposed model, a holistic security check of the complete organization will also be performed after which we will safely be able to say that the said organization is now operating in a secure BYOD environment.

We have talked a lot about the benefits and drawbacks of the BYOD approach, however, there should be a thorough assessment of the risks involved in adopting this approach with which we should be able to decide whether this approach is worth adopting or not. To wrap up our literature review, we would like to discuss a research carried out to identify the exact seriousness of the risks involved in adopting the BYOD approach. To investigate this further, [18] was a very recent research that was conducted in 2020.

This research began with highlighting the benefits of using a single device for both personal and professional work out of which ease, flexibility, accessibility, increased productivity, and job satisfaction were at the top of the list. However, where there are so many advantages of adopting this approach, there are also very destructive security risks associated with the adoption of the BYOD approach. The biggest challenge that the organizations faced as a result of complying with the BYOD approach was of data protection. We all understand that all the business processes these days solely revolve around data because of which its protection is something which can never be taken for granted.

It has also been mentioned in this paper that as a result of letting the employees bring their personal devices to the workplace, the organizations lost all the control that they had earlier on their own devices. Consequently, they were hindered to apply their best security practices to those devices. Moreover, the third party unlicensed applications installed on the employee-owned devices can also lead to cyber-security attacks. These applications have the potential to download malware on the target device and since that device has the access to the corporate network, the malware can easily penetrate through the network hence infecting all the connected devices.

As far as the recommendations provided in this research are concerned, then designing a sound BYOD security policy was at the top of the list. This research also suggested that one single security solution cannot cater to all the security issues. Therefore, we need to direct our efforts to the technical, behavioral, and organizational security control measures at the same time. Furthermore, it is mentioned in this research that in order to stay ahead of the cyber-security attacks, we need to develop intelligent and proactive security risk management solutions along with the BYOD policies. Only then we can get the maximum benefits out of the BYOD approach.

2.2 BYOD in Information Technology(IT) Sector

We all understand the pace at which Information Technology (IT) is progressing these days. New research and development takes place literally every other day. If today, you feel like you are a master of one technology and in that credulity, you stop learning new things, then tomorrow, surely you are going to be left far behind in the race of technology and you will feel like you were never even familiar with these kinds of advancements. That is why, it is advised to us especially these days that we should always keep ourselves up to date.

This is exactly why the IT industry also started paying attention to BYOD once this technology started gaining momentum throughout the globe. Since we all know that the individuals belonging to this particular sector are expected to be ahead of everyone else in playing around with new technology, that is why the IT specialists started putting their efforts into the research in BYOD domain. In the very same regard, [19] highlights the BYOD issues and the strategies put into place by the IT organizations that wish to adopt or have already adopted this practice.

This study was conducted with the organizations of the Mid-Western region to know about all the policies and strategies that have been devised by those organizations to cope with the BYOD security issues. The data for this research was collected by designing and distributing a questionnaire among the participants of the target organizations. The questions in this questionnaire were designed with respect to four different categories i.e. Information about the Participants, Information about the Organization, Participant's Knowledge related to BYOD, and Participant's Experience with BYOD.

These categories comprised of Yes/No and Likert Scale type questions. The sample size for this study was 52. With the responses of this study, the researchers managed to know about the perceptions of the organizational managers regarding their respective BYOD policies. Surprisingly, out of all the participating organizations of this research, only 27% of them supported BYOD. This research highlighted that in order for BYOD to be effective, mobile device management (MDM) software was needed to be purchased by the respective organizations.

Furthermore, this research suggested that proper BYOD policies should be put into place by the organizations that wish to adopt this approach. In addition to creating such policies, they should also be enforced correctly. Along with that, employee training regarding the effective usage of BYOD is also mandatory. If we talk about the shortcoming of this research, then it was done with a very small sample size because of which the results were a little too biased.

Apart from the BYOD security issues, the perceptions of all those organizations who have already adopted this approach also need to be studied. [20] depicts a research carried out in Malaysia with those IT organizations in the public sector that have already embraced BYOD. This study aimed to explore whether the usage of personally owned devices at the workplace can help in the enforcement of green computing or not. A qualitative analysis approach was adopted for this study with interviews as the main data collection method.

Although this research was mainly carried out with the IT departments of the selected organizations, however, within those IT departments, two different groups of participants were chosen. The first group of participants were from the management background whereas the second group of participants were from the technical background. The reason behind selecting these two groups was that the first group is involved in policy making and also all the major decisions of the organization are approved by this group. On the other hand, the latter group is responsible for the implementation of any new technology within an organization.

This research managed to figure out some concerns of the organizations regarding the adoption of BYOD. Firstly, this approach was already practiced within the selected organizations but most of them lacked a proper policy formulation. Secondly, the employees of these organizations did realize that the adoption of BYOD can lead to the development of green computing but the absence of a sound implementation model caused hindrances in this regard.

2.3 BYOD in the Medical Sector

The adoption of BYOD in the medical sector is still something that is under construction. The reason behind us saying that is the medical sector or more precisely, the hospitals deal with critical patient's data which can prove to be fatal for them if it is mishandled in any way. We all understand that the concept of BYOD still has a very long way to go and there are also certain flaws associated with it that are still needed to be fixed. Because of this, we can simply not say to a healthcare professional to use his/her personal devices at workplace for whichever purpose he/she wants and whichever way he/she likes.

It means that a proper mechanism should be devised after which we will be able to safely say that we can now employ the BYOD practice completely throughout the medical sector. To throw light on the current status of BYOD in the healthcare industry of Pakistan, [21] was a research conducted in 2017 focusing on the adoption of BYOD in the hospitals of Pakistan. Before this study, the researchers in Pakistan were silent about the emergence of this approach within the medical sector. Therefore, this study aimed to fill this gap in literature.

The motivation of this research was to investigate the perceptions of the doctors regarding the adoption of BYOD within the different hospitals of Pakistan. With this investigation, the researchers intended to outline all those factors that should be considered while employing this practice within the healthcare sector. Also, based on these highlighted factors, a conceptual model was proposed following which one can ensure healthcare security while complying with the BYOD approach.

The main methodology adopted for this research was divided into two different phases i.e. Identification of BYOD Adoption Factors and Building of a Conceptual Model for BYOD in Healthcare. This research was based on the opinions of doctors and the data gathered through an extensive literature review. However, the model proposed in this research was solely theoretical, which is why a future research was needed that can actually implement this model to validate its effectiveness in the actual hospital settings in Pakistan.

Apart from Pakistan, there are some other countries around the globe too who have contributed to the development of literature in this domain. Out of these countries, USA and Australia are at the top. [22] was one such research carried out in Australia to study the hospital security issues related to BYOD and their corresponding mitigation strategies. This research emphasized on this fact that although the adoption of BYOD has brought about numerous benefits, however, the compliance of this approach within the healthcare sector also meant that the patient's sensitive data was always at a risk.

We know that hospitals deal with critical patient's information also known as Personal Health Information (PHI). Whenever a device's control goes outside the boundaries of a hospital, the PHI is always vulnerable to security threats and data leakage. This research was based on a literature review to highlight all the BYOD security issues within hospitals and also the mitigation solutions that have been put into place so far. After doing that, this research further considered the BYOD Security Framework along with the People Policy Technology (PPT) Model to align the mitigation solutions with the corresponding security issues for their effective implementation.

This research threw light on the fact that although a security framework can present us with all those solutions through which we can tackle with the security issues, however, the usability of these security solutions should also be given due importance. In other words, there should be a proper balance between usability and security for the mitigation solutions to be effective. In this regard, the PPT model plays a very significant role. We need a technology to deal with the ongoing issues but on the same side, we also need a policy that can help in the enforcement of that technology after its implementation. Having said that, if we will still neglect the human behaviour and psychology in this whole process, then both the technology and policy will fail to deliver the desired results.

This is why this research envisaged that all three of them i.e. People, Policy, and Technology should go hand in hand even when the implementation of BYOD should be considered. This research managed to highlight five different security issues namely: Issues Related to Access Control, Data Security Issues, Network Security Issues, Managerial Issues, and Legal Issues. To address these issues, this research came up with a seven phase mitigation model whose main stages were: Planning, Identification, Protection, Detection, Response, Recovery, Assessment and Monitoring respectively,

Now, when we talk about the limitations and future directions of this study, then the mitigation model proposed in this research was solely based on the literature review, therefore, this model should actually be implemented within the hospitals to check its effectiveness. Then we all understand that even the healthcare industry of all the countries out there differ from one another. Since this research was carried out in Australia, therefore, without taking proper control measures, the suggested model cannot be adopted in any other country's healthcare industry.

2.4 BYOD in the Military Sector

Military is yet another sector that holds a very crucial value. In fact, it is actually the sector from which the domain of Information Security emerged for the very first time. The data that this sector works with and produces is so critical that it is enough to destroy a whole nation if it is misused, lost or stolen. That is why, the individuals belonging to this particular sector were quite hesitant with the adoption of BYOD.

[23] was a research conducted to explore the management of mobile devices in the sectors with a highly critical infrastructure such as Military. The criticality of this sector is not a hidden thing and when personal devices are used within this sector for accessing corporate network, then the data of this sector is always at a risk. This research first talked about the security issues within sectors having a critical infrastructure by taking a look at the literature. Then, it highlighted some directions in which the researchers have put in their efforts for tackling with these issues.

This research mainly presented four different solutions for dealing with the BYOD security issues within the critical infrastructure sectors. These solutions were related to: Access Control, Next Generation Firewalls, BYOD Control Models, and BYOD Management and Policy Making Mechanisms. The main finding of this research was that although we are in a dire need of a relatively newer security solution such as Next Generation Firewalls, however, on the same side, we can still not abandon using the traditional access control mechanisms. Secondly, for any security solution to work properly, a sector should first realize and accept itself critical if it really is.

Apart from the critical infrastructure sectors in general, if we talk about the usage of personal devices within the Military educational institutions in particular, then we have a sufficient ground to talk about the experience of individuals belonging to this particular sector. To elaborate this thing further, [24] presents us with a study carried out in Virginia in 2019. This study dealt with the experiences of the Military instructors with their students using personal devices at their respective educational institutions.

The main goals of this research revolved around a single research question i.e. what was the experience of the Military instructors when they allowed their students to incorporate their personal devices for their daily learning activities. To answer this question, this research fundamentally explored how the Military instructors reshaped their teaching methodologies to embrace BYOD effectively. This study was carried out with 12 Military instructors who essentially allowed the usage of personal devices to their students within their classrooms.

The main data collection instruments for this research were qualitative surveys, interviews, and focus groups study with the selected set of participants. Once the responses from all these instruments were collected, they were analyzed while making use of the thematic analysis. The main themes that emerged out as a result of this analysis were related to the attributes of the Military instructors, the overall BYOD culture and the authority of the students built as a result of using personal devices within their classrooms.

Now, talking about the shortcomings of this research, it was carried out only with the male Military instructors. The inclusion of the opposite gender might also make an impact in the study results. Secondly, the sample size for this study was very small because of which the results found in this study cannot be considered reliable. Lastly, this research was based only on the qualitative data. Therefore, some quantitative type questions should have also been added to this study to refine it a bit further.

2.5 BYOD in the Financial Sector

The acceptance of BYOD in the financial sector or more specifically in banks did not come as a surprise since people in every country out there depend on the banks for investments, money exchanges, financial transactions and all other tasks like that. We can safely say that banks form the backbone of a country's economy. Similarly, the banks in Pakistan also hold a very crucial value for us. Now, when we have realized that this is such an important industrial sector of our country, we should have a mechanism for the efficient working within this sector. That is why, the individuals belonging to this particular sector started paying attention towards the adoption of BYOD within banks.

Now, there are also various concerns that come into play with the adoption of this approach within the banks. These concerns are associated with all the reservations that people face as a result of giving a thought to employing BYOD practice within the financial sector. [25] highlights all those concerns by conducting a study with five different financial institutions. Four out of them were banks whereas the fifth one was an insurance company. We all understand that banks deal with highly crucial and personal customer data because of which they are generally hesitant towards the adoption of BYOD.

This research is based on a qualitative data analysis approach which is done on the data collected through semi-structured interviews of 8 different participants belonging to the different managerial positions of the target organizations. This study came up with three main deciding factors that are to be considered before adopting the BYOD approach within the financial institutions. These factors are: Technology, Organization, and Environment. If we try to integrate all these factors together, then we can say that when the innovation seems complex or the proposed technology seems expensive, its benefits are not perceived in a way they should have been perceived otherwise.

If we talk about the above-mentioned three factors separately, then each of them is sub-divided into multiple categories. Technology is divided into Cost, Complexity of Implementation, and the Privacy and Security that it provides. Organization is divided into the Support of Top Level Management and the Culture that is followed throughout the organization. Environment is divided into the Rules and Regulations set up by the government and their compliance, the Competitors of the said organization, and the overall ICT Infrastructure that prevails throughout the whole country.

In a nutshell, the main findings of this research were that the perceived cost that is associated with the implementation of technology can prove to be a hindrance in its adoption. In addition, most of the participants were of the view that BYOD is not a complex technology as far as its implementation is concerned. All the participants agreed on the fact that the cooperation of top level management in the sound implementation of BYOD is a necessity. However, most of the participants expressed that the BYOD approach can become complex to adopt if we start paying too much attention to the privacy and security solutions since there is a large diversity in the type of personal devices that the employees use within an organization.

Overall, this research presented a nice overview of all the factors that are to be considered before the adoption of BYOD within an organization, however, this research also had several limitations associated to it. Firstly, some of the participants of this research belonged to such organizations who have not even adopted BYOD because of which their knowledge regarding this approach was very naive. Secondly, this research revolved only around the South African financial institutions because of which it cannot be generalised.

Whenever a new technology is adopted, there is a visible change that can be seen in the work patterns of the employees of an organization. Similarly, if an organization tends to adopt BYOD, then there will be remarkable changes in the overall working of that organization. To address these changes along with the improvements that can be made in the BYOD policies to enhance the overall BYOD adoption experience, [26] also follows a qualitative data analysis approach. This research also revolves around the different financial institutions of South Africa. The main instruments of data collection used in this research were interviews and surveys with 15 and 87 participants respectively.

This research sheds light on the basic understanding of an organization which has already adopted the BYOD approach. Such organizations perceive BYOD as such a scheme that can help in increasing the organizational productivity, enhancing the working flexibility, strengthening the control, along with a significant cost reduction. However, the organizations with which this particular research was conducted did not have a proper BYOD policy in place or they lacked some very important features because of which they could not be considered strong enough to deal with the changing paradigm that emerged as a result of BYOD adoption.

Along with that, this research presented six different parameters against which the impact of BYOD can be assessed within an organization. These parameters include: Change in the behavior of employees, Work-related motivations of the employees, Influence on the performance of employees, Impact on the workload assigned to the employees, Change in the work patterns of the employees, and the Industrial requirements. Keeping in view all these parameters, this research suggested a re-definition of the work patterns and the policy making within the financial institutions of South Africa.

The findings of this research also revealed that although BYOD is gradually adopted within the financial institutions, however, its usage is mainly restricted to the top level management and it is not allowed for the junior employees. In this kind of BYOD implementation, the organizations could not enjoy the benefits of this approach to the fullest. As far as the limitations of this research are concerned, then there were differing maturity levels of the organizations with which this research was conducted. Secondly, the sample size for the interviews was very small.

Once BYOD is implemented within an organization and a proper BYOD policy is also put into place, the next big challenge that the organizations face are the security issues and vulnerabilities that arise because of this approach and also the policy compliance issues. [27] presents us with a research that was carried out with the banking sector in Indonesia in 2019. This research was based on the responses collected through online questionnaires. There were a total of 31 respondents who took part in this research out of which 24 were from an IT background working in the banks of Indonesia whereas 7 were also from an IT background but working in the non-banking sectors.

This questionnaire consisted of Likert Scale type questions that were meant to gather user's perceptions about the importance of various security controls. On the basis of these responses, this research managed to highlight 20 different security controls that can prevent from the security issues that can potentially arise as a result of adopting

BYOD within the financial sector. This research also suggested that these security controls must be given due consideration while designing a strong BYOD privacy and security policy. Furthermore, this research highlighted that the BYOD security issues arise mainly due to the dual usage of the personal device i.e. for personal as well as professional usage.

Now, if we talk about the limitations of this research, then the security controls presented in this research mapped only on to the seven most commonly occurring security issues. Therefore, there were some other security issues too that still remained unattended. Secondly, the proposed security controls mainly focused on the policy making and human behavior aspects of BYOD implementation whereas the technological aspect of BYOD implementation was not given due importance.

[28] also presents us with a research that was carried out to tackle the issues that arise due to the adoption of BYOD in the banking sector of Nigeria. The goal of this research was the development of a security framework for BYOD enabled banking environments. To achieve this goal, a study was conducted using questionnaires and interviews with 380 and 12 respondents belonging to 4 different banks of Nigeria respectively. Both of these research instruments comprised of open-ended as well as closed questions.

To analyse the quantitative data, SPSS was used whereas for the analysis of the qualitative data, the thematic analysis approach was adopted. As a result of this analysis, this study managed to propose a three dimensional security framework for BYOD enabled banking environments. This framework consisted of the potential BYOD threats, their possible solutions, and all the activities that are needed to be carried out by the individuals and the organization for tackling with these threats. The threats presented in this framework mainly belonged to three different categories namely Social, Technical, and Mobility.

Overall, this research suggested that in order to accommodate the BYOD approach within the financial sector, the existing security practices along with policy formulation need to be redefined. Moreover, the implementation of this three dimensional security framework alone cannot serve the purpose rather periodic employee training on BYOD usage and implications also needs to be carried out. Also, the employees strictly need to comply with the BYOD usage guidelines laid down by their respective organizations.

This research also emphasizes that the employees need to be well aware of the third party device usage. Apart from that, they should be vigilant enough to report to the concerned authorities immediately in the event of a stolen or lost personal device that had access to the corporate data. Employees should also bring this in the knowledge of their respective organizations whenever they wish to change their obsolete devices that they were earlier using for their work-related tasks.

For protecting their critical data, they should be smart enough to maintain its regular backups. Organizations should also provide a list of all the approved applications that the employees are allowed to install on their personal devices. As far as the limitations of this study are concerned, then this research is carried out only with the banks of Nigeria because of which its results cannot be generalized. Secondly, the solutions provided in the proposed three dimensional security framework only caters to the organizational security issues while neglecting the customer's or employee's privacy related issues.

Chapter 3

Research Methodology

Our study design followed both the qualitative and quantitative approaches for gathering and analyzing the data. In this regard, several survey questions were formulated which will be discussed later. Along with the responses to those survey questions, the participants were also asked to provide some demographics related information so that it is easier to contact them later for any follow-up studies (if needed).

Throughout the study, we used one independent variable which was the "Sector" to which the respondent belonged out of Military, IT Industry, Finance, and Hospitals of Pakistan. All of our dependent variables were equated with respect to this one independent variable. Our research methodology is roughly divided into four different sections namely: **Sampling Methodology**, **Data Collection Methodology**, **Data Analysis Methodology**, and **Survey Questions**. We will be discussing all of these sections one by one below:

3.1 Sampling Methodology

For this research, we aimed to collect data from all of our four selected sectors i.e. Military, IT Industry, Finance, and Hospitals of Pakistan. Initially, our plan was to recruit equal number of participants from all the target sectors of Pakistan, however, due to the current situation that emerged as a result of COVID-19, it was quite challenging to maintain this balance. That is why, there is a slight variation in the number of participants that we managed to recruit from each of the four selected sectors. However, the total number of participants for our study was **195**. The exact sector-wise breakdown of the number of participants is shown in the chart below: (see Fig. 3.1).

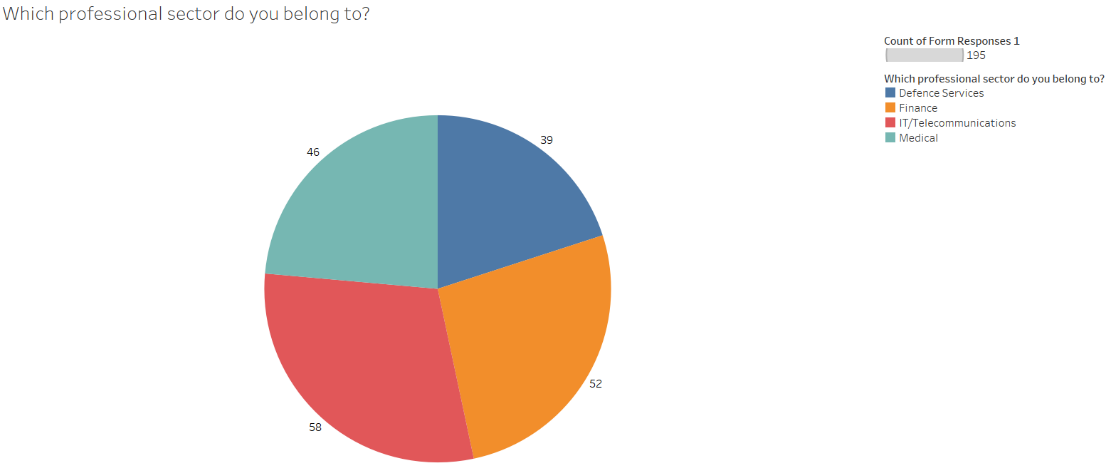


Figure 3.1: Sector-wise breakdown of the number of participants

You can also take a look at the sector-wise breakdown of the percentage of participants in the chart that follows: (see Fig. 3.2).

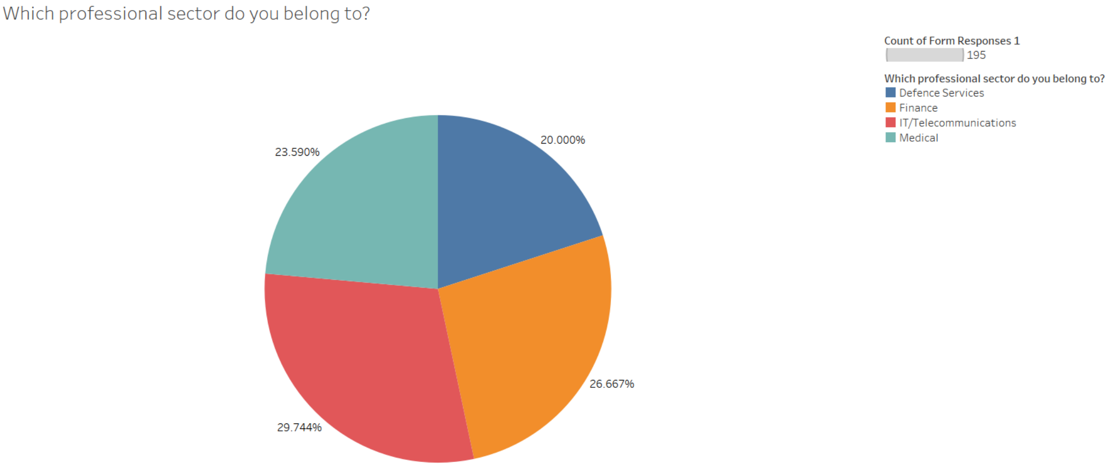


Figure 3.2: Sector-wise breakdown of the percentage of participants

As far as the sampling methodology for the participants of this research is concerned, we first tried to reach out the target organizations via their official emails. However, we could not achieve much success in this regard as a result of which we had to contact our acquaintances working in those organizations directly to get a good number of participants for our study. We approached the participants via their LinkedIn profiles or even through their personal contact numbers.

The participation in this research was voluntary which means that the contacted participants had the full liberty to opt-in or out of this research. The selection criteria of the participants was their easier availability and convenience. This is also known as "Convenience Sampling" as mentioned in [5]. Since the survey designed for this research was quite lengthy, therefore, the convenience sampling approach was best suited for participant selection since it reduces the cost and time and increases accessibility. Moreover, the participants that we recruited for this research were a combination of senior, mid-level, and junior employees to get a broader and clearer picture of their perspectives.

3.2 Data Collection Methodology

For carrying out this study and collecting the relevant data, we designed an extensive survey on Google Forms. This survey contained questions belonging to different categories such as **Demographics Questions**, **Open-Ended Questions**, **Likert Scale Type Questions**, **Multiple Choice Questions**, and **Checkbox Questions**. Providing the answers to all of these questions was made mandatory so that we may not miss out on any important information. Also, since the survey was quite lengthy, that is why maintaining the participants' complete attention was necessary throughout the survey. To achieve this goal, we have added **Attention Check Questions** after predefined intervals throughout the survey.

For making the whole study easier for the participants to understand its goals and our overall objectives, a short summary about this research was provided at the very beginning of our survey. Moreover, since we intended to explore the perspectives (regarding BYOD) of the participants belonging to such diverse backgrounds, that is why we also provided one-liner descriptions wherever needed with the terminologies that we thought might be unfamiliar to the participants. The link to our survey is as follows: https://forms.gle/d3ddTRiaPCMVSvy58

If we try to further dig down into the actual flow of our survey, then based upon the responses of the first few questions of the survey, there were three different channels. The first channel was for the participants whose organizations have faced a security issue as a result of complying with the BYOD approach, the second channel was for the ones who have not faced any such issues so far, whereas the third channel was for the participants whose organizations have not adopted the BYOD approach as yet. Each question was modified according to the context and the background from which the participant was coming.

3.3 Data Analysis Methodology

Since our data was both qualitative and quantitative, therefore, to analyze it well, we had to employ both the qualitative and quantitative data analysis approaches. For the qualitative data, we made use of the "Thematic Analysis". We first coded all the responses to the qualitative questions into relevant themes so that the data becomes easier to analyze. After that, we have discussed the themes related to every single qualitative question in detail in our Analysis and Results section.

As far as the quantitative data is concerned, then there were three different classes of questions whose responses came into this category. For the first two classes of questions, we made use of the "Statistical Analysis" whereas for the third class of questions, we relied on the charts produced by Google Forms. The first class of questions produced the results that were "categorical" or the nature of dependent variable in such relations was "categorical". That is why, we employed the "Chi-Square" test in R to analyze all such data. For the second class of questions, the nature of the dependent variable was "interval" as a result of which we applied "Kruskal Wallis" test in R to analyze all such data.

The third class of questions had dependent variables that were neither categorical nor interval. Rather those were the questions in which the participants were allowed to select multiple options. That is why, to analyze all such data, we made use of the histograms and bar graphs in Google Forms to have a clear picture about the responses from each of the four sectors. Once all the relevant tests were carried out and all the respective graphs, tables or charts were created, a clear comparison was drawn between the responses of all four sectors. This will be discussed in depth in our Analysis and Results section.

3.4 Survey Questions

For investigating the current state of BYOD in the four different industrial sectors of Pakistan and for answering our high-level research questions, we formulated some survey questions on the basis of which we have collected and analyzed our data. The quantitative survey questions were as follows:

- **SQ-1:** Is the BYOD practice allowed in your organization or not?
- **SQ-2:** Does a dedicated BYOD policy exist in your organization or not?
- **SQ-3:** Despite the dis-allowance of BYOD practice or non-existence of a BYOD policy, do you still take any personal device to the workplace?
- **SQ-4:** Do you share the login credentials of your personal device with anyone?
- **SQ-5:** Do you use two factor authentication for securing your personal device?
- **SQ-6:** Do you connect your personal device with a freely available insecure Wi-Fi?
- **SQ-7:** Do you use encryption for protecting your data residing in your personal device?
- **SQ-8:** Has your organization ever faced a security issue as a result of adopting the BYOD approach?

- **SQ-9:** Do you think that BYOD approach can pose to be a threat for your organization in the future?
- **SQ-10:** What is your opinion on abandoning the BYOD approach for preventing the security issues that can arise because of this approach?
- **SQ-11:** How would you rate the implementation of your organization's BYOD policy?
- **SQ-12:** Which personal device do you use at the workplace?
- **SQ-13:** Which applications do you use the most on your personal device at the workplace?
- **SQ-14:** In your opinion, which security controls are the most important for protecting the data residing on your personal device?
- **SQ-15:** In your opinion, what are the most important BYOD security policies?
- **SQ-16:** In your opinion, what are the challenges faced by the employees while complying with an organization's BYOD policy?

The qualitative survey questions are stated below:

- **SQ-17:** Share how you have been using your personal device at the workplace without bringing it to anyone's knowledge.
- **SQ-18:** Describe your experience of shifting from the traditional approach to the BYOD approach. (Corresponds to RQ-1)
- **SQ-19:** Explain the BYOD practices employed by your respective organization for avoiding the BYOD security issues. (Corresponds to RQ-3)
- **SQ-20:** In your opinion, what are the differences between the traditional and BYOD approach? (Corresponds to RQ-1)
- **SQ-21:** Suggest some possible improvements in the implementation of BYOD for strengthening its security. (Corresponds to RQ-3)
- **SQ-22:** Explain the BYOD security issue[s] in a few words (if your organization has faced any). (Corresponds to RQ-2)

- **SQ-23:** What was the strategy employed by your respective organization for tackling with the BYOD security issue[s]? (Corresponds to RQ-3)
- **SQ-24:** What are the differences between the traditional and BYOD approach that give rise to the security issues? (Corresponds to RQ-1)
- **SQ-25:** Which BYOD issues still remain unattended within your respective organization? (Corresponds to RQ-4)
- **SQ-26:** Justify your opinion on abandoning the BYOD approach for avoiding the security issues.

The last four qualitative survey questions were for the organizations who are not practicing BYOD currently:

- **SQ-27:** In your opinion, what are the differences between the traditional and BYOD approach? (Corresponds to RQ-1)
- **SQ-28:** What are the security issues that can possibly arise as a result of following the BYOD approach? (Corresponds to RQ-2)
- **SQ-29:** What are the differences between the traditional and BYOD approach that give rise to the security issues? (Corresponds to RQ-1)
- **SQ-30:** Justify your opinion on abandoning the BYOD approach for avoiding the security issues.

We have tried to answer these survey questions with respect to all the four selected sectors through our study.

Chapter 4

Analysis and Results

Note: The "sector" variable which is our independent variable had four possible values i.e. "IT/Telecommunications", "Defence Services", "Medical", and "Finance". We will be using the same independent variable for all of our survey questions i.e. for both quantitative and qualitative.

Since we collected both the quantitative and qualitative data from our selected participants, therefore, the analysis of both types of data is discussed in the following sections:

4.1 Quantitative Data Analysis and Results

As we have already mentioned that we made use of the Statistical Analysis for our quantitative data, therefore, before actually proceeding with our quantitative data analysis and their respective results, we would like to discuss the tests that we performed briefly. But even before that, we will state the reason of selecting these tests. Whenever we have one independent variable and it has two or more independent groups or levels, then we apply Chi-Square test if the nature of the dependent variable is categorical and Kruskal Wallis test if the nature of the dependent variable is interval or ordinal.

If we talk about these tests a little more, then the Chi-Square test is used to tell if the correlation between the independent and dependent variable is significant or not. In the results of a Chi-Square test, the threshold p-value is **0.05**. If the p-value of our test is less than the threshold value, then we say that there is a significant correlation between our variables under discussion, otherwise, not. Through the Kruskal Wallis test, our aim is to check whether there are significant differences among the groups or not.

Again, in the case of the Kruskal Wallis test, if the p-value is less than **0.05**, then we can say that there are significant differences among the groups, otherwise, not. However, we need to go one step further if the p-value is less than 0.05 in case of this test. It is so, because we still will not know exactly that which of the groups under discussion are responsible for this difference. For that, we use a post-hoc test known as the "Dunn's Test". This test performs pair-wise comparisons of the different groups and tells exactly which groups differ from each other.

The quantitative data analysis and results of all of our quantitative survey questions have been discussed in the sections below:

4.1.1 SQ-1: Is the BYOD practice allowed in your organization or not?

For this survey question, we performed Chi-Square test on the variables "sector" and "practice". The former one is independent whereas the latter one is dependent variable. The "practice" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **0.001719** which is less than **0.05**. It means that there is a significant correlation between our dependent and independent variables.

When we further tried to analyse these results by looking at the exact values from each sector by creating a matrix in R, then we came to know that the dominant response for SQ-1 for the Defence Services and Finance sectors was **No** whereas for IT/Telecommunications and Medical sectors was **Yes**. It means that the BYOD practice is allowed in most of the surveyed organizations belonging to the IT/Telecommunications and Medical sectors whereas it is mostly disallowed in the Defence Services and Medical sectors.

4.1.2 SQ-2: Does a dedicated BYOD policy exist in your organization or not?

For this survey question, we performed Chi-Square test on the variables "sector" and "policy". The former one is independent whereas the latter one is dependent variable. The "policy" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **0.0002628** which is less than **0.05**. It means that there is a significant correlation between our dependent and independent variables.

When we further tried to analyse these results by looking at the exact values from each sector by creating a matrix in R, then we came to know that the dominant response for SQ-2 for the Defence Services sector was **Yes** whereas for the rest of the three sectors was **No**. It means that most of the respondents from the Defence Services were of the view that dedicated BYOD policies exist in their respective organizations whereas for the other three sectors, such policies were non-existent.

4.1.3 SQ-3: Despite the dis-allowance of BYOD practice or non-existence of a BYOD policy, do you still take any personal device to the workplace?

For this survey question, we performed Chi-Square test on the variables "sector" and "disallow". The former one is independent whereas the latter one is dependent variable. The "disallow" variable corresponds directly to our survey question. This question had two possible answers i.e. "Yes" and "No". The p-value that we obtained for this Chi-Square test was **6.977e-05** which is extremely smaller than **0.05**. It means that there is a significant correlation between our dependent and independent variables.

When we further tried to analyse these results by looking at the exact values from each sector by creating a matrix in R, then we came to know that the dominant response for SQ-3 for the Defence Services and Finance sectors was **No** whereas for IT/Telecommunications and Medical sectors was **Yes**. It means that the respondents from the Defence Services and Finance sectors were not taking their personal devices to the workplace if the BYOD practice was disallowed or the BYOD policy was non-existent whereas, it was vice-versa for the IT/Telecommunications and Medical sectors.

4.1.4 SQ-4: Do you share the login credentials of your personal device with anyone?

For this survey question, we performed Chi-Square test on the variables "sector" and "login". The former one is independent whereas the latter one is dependent variable. The "login" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **0.2964** which is larger than **0.05**.

It means that for SQ-4 there is no significant correlation between our dependent and independent variables which means that we have failed to reject the null hypothesis for this particular survey question. In other words, we can say that the responses to this question do not vary significantly with respect to the sector. However, for this particular question, most of the respondents from all the four sectors selected the "No" option i.e. they do not share the login credentials of their personal devices with anyone.

4.1.5 SQ-5: Do you use two factor authentication for securing your personal device?

For this survey question, we performed Chi-Square test on the variables "sector" and "twoFA". The former one is independent whereas the latter one is dependent variable. The "twoFA" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **0.4929** which is larger than **0.05**.

It means that for SQ-5 there is no significant correlation between our dependent and independent variables which means that we have failed to reject the null hypothesis for this particular survey question. In other words, we can say that the responses to this question do not vary significantly with respect to the sector. However, for this particular question, most of the respondents from all the four sectors selected the "Yes" option i.e. they use two factor authentication for securing their personal devices.

4.1.6 SQ-6: Do you connect your personal device with a freely available insecure Wi-Fi?

For this survey question, we performed Chi-Square test on the variables "sector" and "wifi". The former one is independent whereas the latter one is dependent variable. The "wifi" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **3.702e-05** which is extremely less than **0.05**. It means that there is a significant correlation between our dependent and independent variables.

When we further tried to analyse these results by looking at the exact values from each sector by creating a matrix in R, then we came to know that the dominant response for SQ-6 for the Medical and Finance sectors was **Yes** whereas for the IT/Telecommunications and Military sectors was **No**. It means that most of the respondents from the Medical and Finance sectors were habitual of connecting their personal devices with freely available insecure Wi-Fi whereas a majority of the respondents from the other two sectors were avoiding this practice.

4.1.7 SQ-7: Do you use encryption for protecting your data residing in your personal device?

For this survey question, we performed Chi-Square test on the variables "sector" and "encrypt". The former one is independent whereas the latter one is dependent variable. The "encrypt" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **0.457** which is more than **0.05**. It means that for SQ-7 there is no significant correlation between our dependent and independent variables which means that we have failed to reject the null hypothesis for this particular survey question.

In other words, we can say that the responses to this question do not vary significantly with respect to the sector. However, for this particular question, most of the respondents from three out of the four sectors i.e. Defence Services, Finance, and Medical selected the "Yes" option i.e. they use encryption for protecting the data residing in their personal devices whereas the majority of the respondents from the IT/Telecommunications sector went with the "No" option.

4.1.8 SQ-8: Has your organization ever faced a security issue as a result of adopting the BYOD approach?

For this survey question, we performed Chi-Square test on the variables "sector" and "secIssue". The former one is independent whereas the latter one is dependent variable. The "secIssue" variable corresponds directly to our survey question. This question had two possible answers i.e. "Yes" and "No". The p-value that we obtained for this Chi-Square test was **0.008362** which is less than **0.05**. It means that there is a significant correlation between our dependent and independent variables.

When we further tried to analyse these results by looking at the exact values from each sector by creating a matrix in R, then we came to know that the dominant response for SQ-8 for the Defence Services was **Yes** whereas for the rest of the three sectors was **No**. It means that most of the respondents from the Defence Services expressed that they had faced a security issue as a result of complying with the BYOD approach whereas it was vice-versa for the rest of the three sectors.

4.1.9 SQ-9: Do you think that BYOD approach can pose to be a threat for your organization in the future?

For this survey question, we performed Chi-Square test on the variables "sector" and "threat". The former one is independent whereas the latter one is dependent variable. The "threat" variable corresponds directly to our survey question. This question had three possible answers i.e. "Yes", "No", and "Maybe". The p-value that we obtained for this Chi-Square test was **0.00643** which is less than **0.05**. It means that there is a significant correlation between our dependent and independent variables.

When we further tried to analyse these results by looking at the exact values from each sector by creating a matrix in R, then we came to know that the dominant response for SQ-9 for the Defence Services and IT/Telecommunications sectors was **Yes** whereas for the Finance and Medical sectors was **No**. It means that most of the respondents from the Defence Services and IT/Telecommunications sectors were of the view that the BYOD approach can pose to be a threat for their organization in future whereas the respondents from the other two sectors thought vice-versa.

4.1.10 SQ-10: What is your opinion on abandoning the BYOD approach for preventing the security issues that can arise because of this approach?

For this survey question, we performed Chi-Square test on the variables "sector" and "abandon". The former one is independent whereas the latter one is dependent variable. The "abandon" variable corresponds directly to our survey question. This question had three possible answers i.e. "I am not sure", "It is a good idea to do that", and "It is not at all practical to do that". The p-value that we obtained for this Chi-Square test was **0.5753** which is greater than **0.05**. It means that for SQ-10 there is no significant correlation between our dependent and independent variables which means that we have failed to reject the null hypothesis for this particular survey question.

In other words, we can say that the responses to this question do not vary significantly with respect to the sector. However, for this particular question, most of the respondents from three out of the four sectors i.e. Defence Services, Finance, and IT/Telecommunications selected the "It is a good idea to do that" option i.e. they preferred abandoning the BYOD approach for avoiding the security issues whereas the respondents from the Medical sector have equally responded in favor of the first and third options.

A summary of the analysis and results of the above **10** quantitative survey questions is also given in the table below (see Table. 4.1). In this table, we have shortened the names of our sectors as **DS**, **F**, **IT/T**, **M** that refer to **Defence Services**, **Finance**, **IT/Telecommunications**, and **Medical** respectively. **S** and **NS** in this table refer to **Significant Correlation** and **Not a Significant Correlation** between the independent and dependent variables respectively. Moreover, in the last row of our table, **NotP** and **NotS** refer to **It is not at all practical to do that** and **Not Sure** respectively.

Questions	Sectors	P-Value	S/NS	Most Common Response
Is the BYOD practice allowed in your organization or not?	DS F IT/T M	0.001719	S	No No Yes Yes
Does a dedicated BYOD policy exist in your organization or not?	DS F IT/T M	0.0002628	S	Yes No No No
Despite the dis-allowance of BYOD practice or non-existence of a BYOD policy, do you still take any personal device to the workplace?	DS F IT/T M	6.977e-05	S	No No Yes Yes
Do you share the login credentials of your personal device with anyone?	DS F IT/T M	0.2964	NS	No No No No

Do you use two factor authentication for securing your personal device?	DS F IT/T M	0.4929	NS	Yes Yes Yes Yes
Do you connect your personal device with a freely available insecure Wi-Fi?	DS F IT/T M	3.702e-05	S	No Yes No Yes
Do you use encryption for protecting your data residing in your personal device?	DS F IT/T M	0.457	NS	Yes Yes No Yes
Has your organization ever faced a security issue as a result of adopting the BYOD approach?	DS F IT/T M	0.008362	S	Yes No No No
Do you think that BYOD approach can pose to be a threat for your organization in the future?	DS F IT/T M	0.00643	S	Yes No Yes No
What is your opinion on abandoning the BYOD approach for preventing the security issues that can arise because of this approach?	DS F IT/T M	0.5753	NS	Good Good Good NotP/NotS

Table 4.1: Summary of the analysis and results of the Survey Questions 1-10. Chi-Square Test was applied in R for all of these questions.

4.1.11 SQ-11: How would you rate the implementation of your organization's BYOD policy?

For this survey question, we performed Kruskal Wallis test on the variables "sector" and "ratingPolicy". The former one is independent whereas the latter one is dependent variable. The "ratingPolicy" variable corresponds directly to our survey question. This question had five possible answers or rating values i.e. "1", "2", "3", "4" and "5" where "1" represents "Excellently implemented" and "5" represents "The policy just exists there. No one really follows it". The p-value that we obtained for this Chi-Square test was **0.002155** which is less than **0.05**. It means that there is a significant difference between the different groups.

To analyse this difference further, we performed the "Dunn's Post-Hoc Test" in R to perform a pair-wise comparison on all the four selected sectors. By performing this test, we came to know that the significant difference that was produced in the results of our Kruskal Wallis test was because of the two pairs i.e. the Defence Services-IT/Telecommunications and the Defence Services-Medical pairs since the p-values for both of these pairs were **0.009836971** and **0.004518933** respectively which are less than **0.05**. It means that the responses for this survey question for the Defence Services and IT/Telecommunications sectors and for the Defence Services and Medical sectors greatly varied from each other. However, most of the participants from all the four sectors selected the "3" value as a response to this question.

Note: For the following quantitative survey questions, we have used the graphical analysis tools provided by Google Forms.

4.1.12 SQ-12: Which personal device do you use at the workplace?

For SQ-12, we presented the participants with four different options and they had the liberty to choose as many out of them as they wanted. These options were "Laptop", "Mobile Phone", "Tablet", and "Other". According to our graphical analysis, we managed to find out that the most preferred personal device of the participants from all the four sectors (combined) was "Mobile Phone" with a preference percentage of **78.6%** whereas the least preferred personal device was "Tablet" with a preference percentage of **9.2%**.

The most interesting fact was that when we asked the same question to the participants whose organizations were currently not practicing BYOD, their personal device preference turned out to be exactly the same i.e. they would also have preferred "Mobile Phone" over other personal devices if they were allowed to use them at the workplace. These results are summarized in the graph below: (see Fig. 4.1)

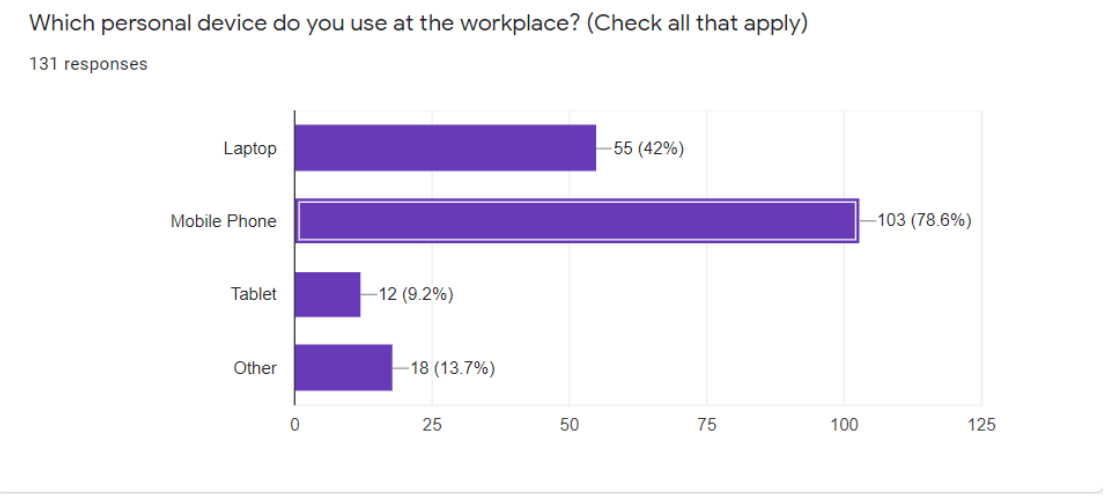
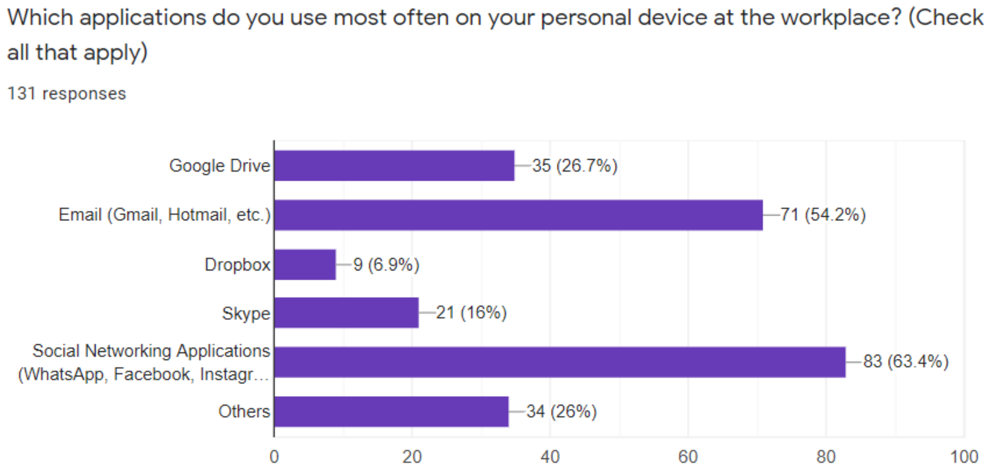


Figure 4.1: Personal device preference of the participants

4.1.13 SQ-13: Which applications do you use the most on your personal device at the workplace?

For SQ-13, we presented the participants with six different options and they had the liberty to choose as many out of them as they wanted. These options were "Google Drive", "Email", "Dropbox", "Skype", "Social Networking Applications", and "Others". According to our graphical analysis, we managed to find out that the most frequently used applications on the personal devices by the participants from all the four sectors (combined) were "Social Networking Applications" such as WhatsApp, Facebook, Instagram, etc. with a usage percentage of **63.4%** whereas the least frequently used application was "Dropbox" with a usage percentage of **6.9%**.

The most interesting fact was that when we asked the same question to the participants whose organizations were currently not practicing BYOD, their applications usage preferences on personal devices turned out to be exactly the same i.e. they would also have preferred using the "Social Networking Applications" on their personal devices instead of any other applications if they were allowed to use their personal devices at the workplace. These results are summarized in the graph below: (see Fig. 4.2)


Which applications do you use most often on your personal device at the workplace? (Check all that apply)

131 responses

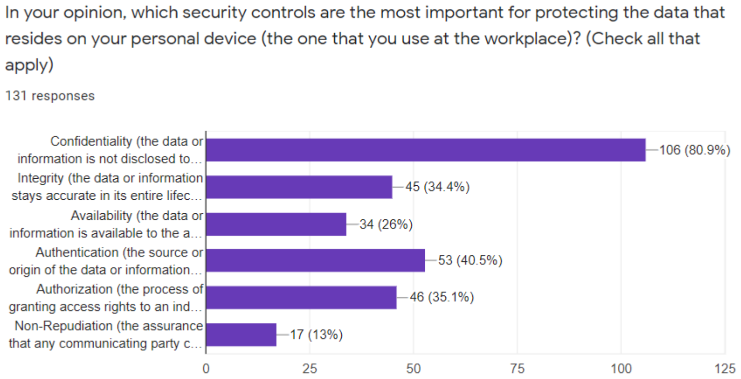
Figure 4.2: Most frequently used applications on the personal devices by the participants

4.1.14 SQ-14: In your opinion, which security controls are the most important for protecting the data residing on your personal device?

For SQ-14, we presented the participants with six different security controls (with a one-liner description of each for making it easier for the participant to understand it) and they had the liberty to choose as many out of them as they wanted. These security controls were "Confidentiality", "Integrity", "Availability", "Authentication", "Authorization" and "Non-Repudiation". According to our graphical analysis, we managed to find out that the most preferred security control of the participants from all the four sectors (combined) was "Confidentiality" with a preference percentage of **80.9%** whereas the least preferred security control was "Non-Repudiation" with a preference percentage of

13%.

The most interesting fact was that when we asked the same question to the participants whose organizations were currently not practicing BYOD, their security control preference turned out to be exactly the same i.e. they would also have preferred "Confidentiality" over other security controls if they were allowed to use their personal devices at the workplace. Another thing that we inferred from our observation was that since "Non-Repudiation" was the least familiar security control for most of our participants, that is why they did not consider to select this security control in their response despite its importance. These results are summarized in the graph below: (see Fig. 4.3)



In your opinion, which security controls are the most important for protecting the data that resides on your personal device (the one that you use at the workplace)? (Check all that apply)

131 responses

Figure 4.3: Security control preference of the participants

4.1.15 SQ-15: In your opinion, what are the most important BYOD security policies?

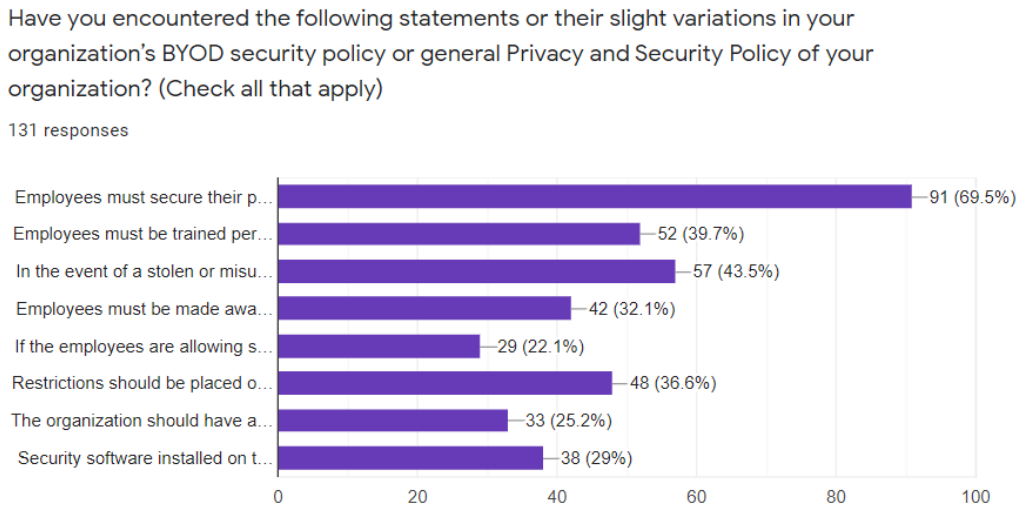
For SQ-15, we presented the participants with eight different BYOD security policies (that we have extracted from our literature review) and they had the liberty to choose all of those policies from them which they have encountered within their respective organizations. These policies are stated below:

- **P1:** Employees must secure their personal devices with strong passwords and two-factor authentication methods wherever possible.

- **P2:** Employees must be trained periodically about the secure usage of personal devices at the workplace.
- **P3:** In the event of a stolen or misused device, employees must immediately report it to the organization to minimize the security risks.
- **P4:** Employees must be made aware of the third-party usage of the applications that they install on the personal devices they use at the workplace.
- **P5:** If the employees are allowing someone else to use their personal devices (the ones that they also use at the workplace), then what precautionary measures they must take before doing so?
- **P6:** Restrictions should be placed on the corporate data that the employees can access with their personal devices.
- **P7:** The organization should have a proper disaster recovery plan in place in case an employee faces a data breach while using his personal device at the workplace.
- **P8:** Security software installed on the employees' personal devices to protect their data must be constantly updated.

According to our graphical analysis, we managed to find out that the most preferred BYOD security policy according to the participants from all the four sectors (combined) was "P1" with a preference percentage of **69.5%** whereas the least preferred BYOD security policy was "P5" with a preference percentage of **22.1%**.

The most interesting fact was that when we asked the same question to the participants whose organizations were currently not practicing BYOD, their BYOD security policy preference turned out to be exactly the same i.e. they would also have preferred "P1" over other BYOD security policies if they were allowed to use their personal devices at the workplace. These results are summarized in the graph below: (see Fig. 4.4)



Have you encountered the following statements or their slight variations in your organization’s BYOD security policy or general Privacy and Security Policy of your organization? (Check all that apply)

131 responses

Figure 4.4: Most important BYOD security policies according to the participants

4.1.16 SQ-16: In your opinion, what are the challenges faced by the employees while complying with an organization’s BYOD policy?

For SQ-16, we presented the participants with seven different challenges that they could potentially face while complying with their organization’s BYOD policy and they had the liberty to choose as many out of them as they considered relevant. These challenges are stated below:

- **C1:** The policy is too technical to be understood by a junior employee.
- **C2:** The rules mentioned within the policy can just not be followed as they impose unnecessary restrictions on the employees.
- **C3:** The privacy policy stays silent on the employee’s privacy and only focuses on the organisation’s security.
- **C4:** There is no check and balance by the senior management on the compliance of the policy.
- **C5:** The policy is just there to be followed by the junior employees and the senior management just do not bother to follow it.

- **C6:** The policy puts the employee's personal data at risk.
- **C7:** Instead of solely relying on a policy, some other technical controls also need to be implemented for ensuring the security.

According to our graphical analysis, we managed to find out that the most commonly faced challenge while complying with the BYOD policies for the participants from all the four sectors (combined) was "C1" with a frequency percentage of **47.3%** whereas the least commonly faced challenge was "C5" with a frequency percentage of **12.2%**.

The most interesting fact was that when we asked the same question to the participants whose organizations were currently not practicing BYOD, their views on the challenges faced while complying with the BYOD policies turned out to be exactly the same i.e. they would also have selected the "C1" challenge as the most commonly faced compliance challenge instead of any other challenges if they were allowed to use their personal devices at the workplace. These results are summarized in the graph below: (see Fig. 4.5)

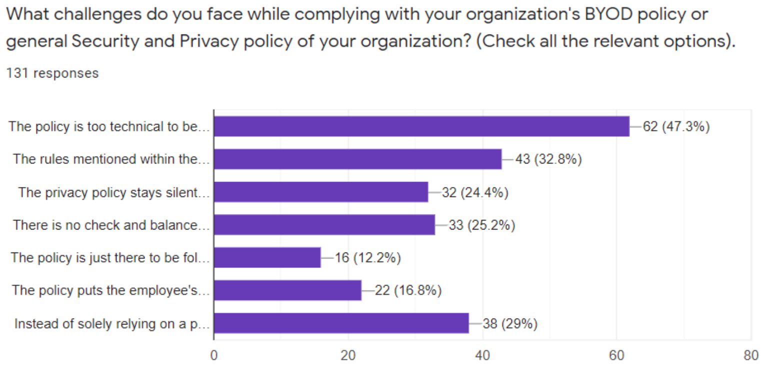


Figure 4.5: Challenges faced by the participants while complying with the BYOD policies

4.2 Qualitative Data Analysis and Results

For the analysis of our qualitative data and the deduction of its results, we have made use of the Tableau interactive data visualization software. We chose this software because it provides professional tools for analyzing both qualitative and quantitative data.

Because of the nature of our qualitative questions, this software suggested us to draw bar graphs for our provided data which will make the sector-wise relationships more easier to visualize. All we had to do was to provide this software with the fields whose values we wanted to analyze along with our main data source and it created all the bar graphs for us.

However, before starting to use this tool for our qualitative data analyses, we had to do some pre-processing for our 14 qualitative questions. Since all the qualitative questions were mainly open-ended, that is why, we first had to code each and every response to these questions manually into relevant themes. For that, we had to read through all the responses to these 14 questions twice after which we managed to device relevant themes for the responses. After doing that, we rechecked the coded data to remove the discrepancies (if any). Finally, after creating these themes, we provided this coded data to Tableau for visualizing the results clearly. The themes that emerged corresponding to all of our 14 qualitative survey questions have been discussed (sector-wise) below:

Note: The following qualitative survey questions are general i.e. they do not correspond specifically to any of our Research Questions.

4.2.1 SQ-17: Share how you have been using your personal device at the workplace without bringing it to anyone's knowledge.

For this survey question, we asked the respondents to share how they had been using their personal devices at workplace without making anyone else aware of this (if the personal device usage is disallowed in their respective organizations or if the BYOD policy is non-existent). The themes that emerged for SQ-17 for our four sectors are shown in the bar graph below: (see Fig. 4.6)

In this bar graph, "Code" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-17. Moreover, we have also discussed these themes sector-wise in the following sections:

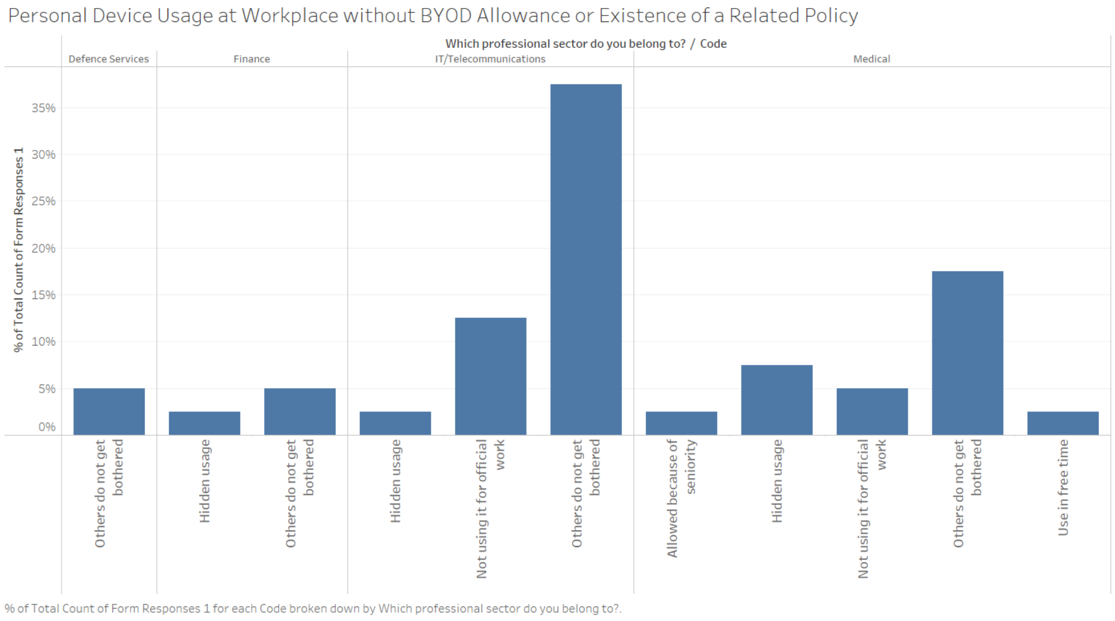


Figure 4.6: Personal Device Usage at Workplace without BYOD Allowance or Existence of a Related Policy

Defence Services:

For this particular sector, the only theme that emerged out with a percentage of **5%** was that "Others do not get bothered". Basically, the respondents were of the view that since the device under discussion is owned by them, therefore, they do not really care if it is allowed to bring it to their workplace or not. They will still continue to use it and no one else would be bothered by it since it is their personal device.

Finance:

For the Finance sector, two different themes emerged out for SQ-17 i.e. "Hidden usage" and "Others do not get bothered" with the percentages of **2.5%** and **5%** respectively. Some of the participants of this sector expressed that they had been doing hidden usage of their personal devices either when no one else was looking or around. Also, the participants with the responses belonging to the second theme had similar views as that of the Defence Services participants.

IT/Telecommunications:

For this particular sector, three different themes emerged out for SQ-17 i.e. "Hidden usage", "Not using it for official work" and "Others do not get bothered" with the percentages of **2.5%**, **12.5%**, and **37.5%** respectively. It means that 12.5% of the participants from this sector were of the view that since they do not use their personal device for official work rather they only keep it with them for personal usage, that is why, it is completely alright to bring those devices at the workplace despite the dis-allowance of BYOD practice or non-existence of a related policy.

Medical:

For the Medical sector, five different themes emerged out for SQ-17 i.e. "Allowed because of seniority", "Hidden usage", "Not using it for official work", "Others do not get bothered", and "Use in free time" with the percentages of **2.5%**, **7.5%**, **5%**, **17.5%**, and **2.5%** respectively. Most of the participants from this sector were using personal devices at the work place because no one else gets bothered if they do so whereas some of them expressed that although this practice is discouraged within there organization, however, they can still use their personal device because of the seniority of their post. Moreover, some of the participants also shared that they use their personal devices when they are free from work because of which they do not get punished for breaking the norms.

4.2.2 SQ-26: Justify your opinion on abandoning the BYOD approach for avoiding the security issues.

For this survey question, we asked the respondents to share the justification of their opinion on abandoning the BYOD approach for avoiding the security issues. The themes that emerged for SQ-26 for our four sectors are shown in the bar graph below: (see Fig. 4.7)

In this bar graph, "Code9" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-26. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The most dominant theme that emerged for SQ-26 for this sector was "Guaranteed Security" with a percentage of **15%**. It meant that the participants who thought of

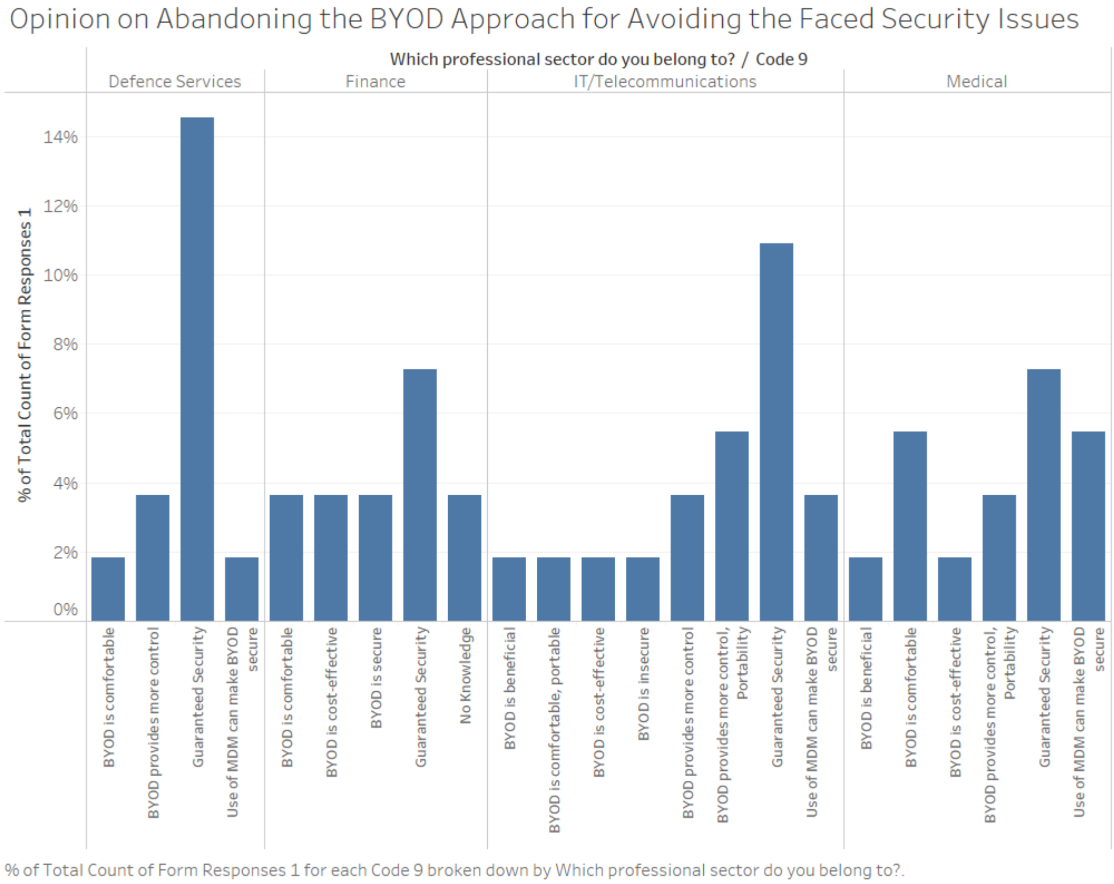


Figure 4.7: Opinion on abandoning BYOD approach for avoiding the security issues

abandoning the BYOD approach as a good measure for avoiding the security issues justified this opinion by expressing that we can guarantee maximum security by using the organization owned devices since securing and managing them centrally is much more convenient. The rest of the participants who considered abandoning BYOD as impractical justified their opinions by calling BYOD as more comfortable, or an approach that provides more autonomy to the employees, or that the usage of a mobile device management (MDM) software can make BYOD secure.

Finance:

The most common theme for SQ-26 for this sector was also "Guaranteed Security" with a percentage of **7.4%**. Apart from this, some of the participants who did not prefer abandoning the BYOD approach considered it to be comfortable, secure, and cost-effective.

IT/Telecommunications:

Again, the dominant theme for this sector for SQ-26 was "Guaranteed Security" with a percentage of **11%**. Some participants from this sector who were in the favor of abandoning BYOD justified their opinion by calling this approach as insecure. On the other hand, the participants who did not prefer abandoning the BYOD approach justified their thoughts by calling BYOD portable, comfortable, beneficial, cost-effective, and an approach that can provide more autonomy to the employees. Moreover, some of them also suggested the use of MDM to make BYOD secure.

Medical:

Yet again, the dominant theme for the Medical sector for SQ-26 was "Guaranteed Security" with a percentage of **7.4%**. The other themes that emerged for this particular sector for the participants who were not in the favor of abandoning the BYOD approach for SQ-26 were the same as that of the IT/Telecommunications sector.

4.2.3 SQ-30: Justify your opinion on abandoning the BYOD approach for avoiding the security issues. (for organizations who are not practicing BYOD currently)

For this survey question, we asked the respondents to justify their opinions on abandoning the BYOD approach for avoiding the potential security issues. Again, this question was designed for the participants whose organizations were not practicing BYOD currently. The themes that emerged for SQ-30 for our four sectors are shown in the bar graph below: (see Fig. 4.8)

In this bar graph, "Code13" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-30. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The only theme that emerged for SQ-30 for this sector was "Use of MDM can make BYOD secure" with a percentage of **18.4%**. It meant that the respondents from this

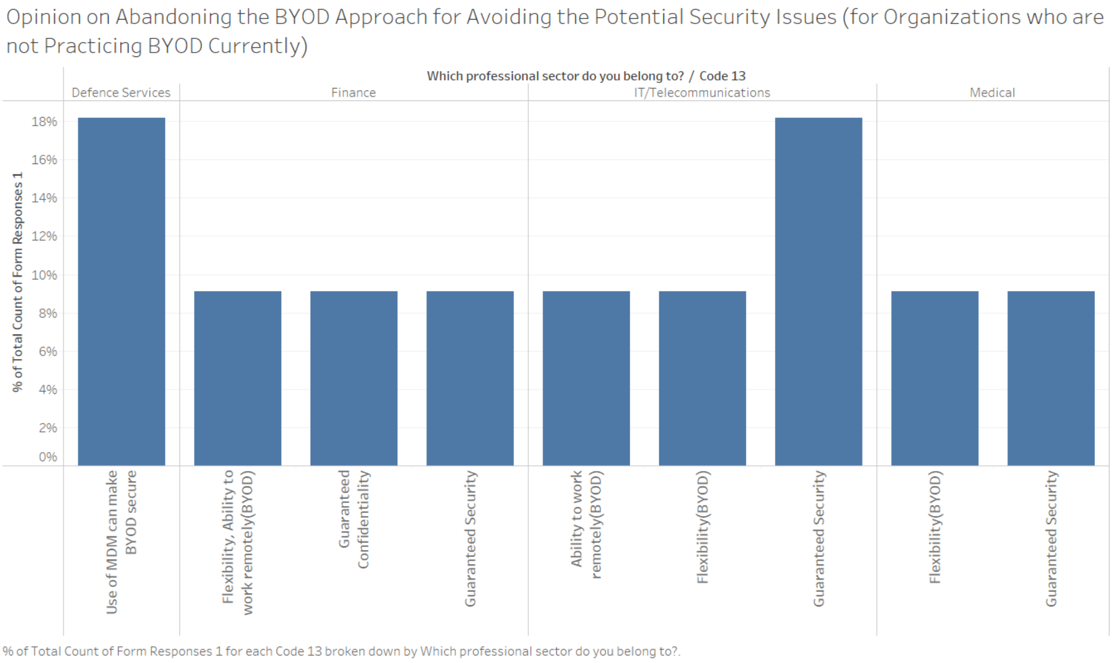


Figure 4.8: Opinion on abandoning the BYOD approach for avoiding the potential security issues (for organizations who are not practicing BYOD currently)

sector were not in favor of abandoning the BYOD approach rather they suggested to use MDM to ensure security while complying with this approach.

Finance:

The three themes that emerged for SQ-30 for this sector had the same percentages i.e. **9.2%**. The participants of this sector who were not in favor of abandoning BYOD justified their opinion by calling this approach as flexible and the one that can provide with the ability to work remotely. On the other hand, the participants who were in favor of abandoning this approach mentioned guaranteed confidentiality and security as the reasons behind their choice.

IT/Telecommunications:

The dominant theme that emerged for this sector for SQ-30 was "Guaranteed Security" with a percentage of **18.4%**. It meant that the participants from this sector who were in the favor of abandoning the BYOD approach attributed guaranteed security to be the reason behind their preference. Moreover, the participants of this sector who were not in favor of abandoning the BYOD approach considered it more flexible and an approach that can provide the ability to work remotely.

Medical:
The two themes that emerged for SQ-30 for this sector were "Flexibility (BYOD)" and "Guaranteed Security" with percentages of **9.2%** each. The first theme was for the respondents who were not in the favor of abandoning BYOD and they justified their choice by calling BYOD flexible. This corresponds to the control, ease and autonomy that the personal devices provide to the employees. On the other hand, the second theme was for the participants who were in favor of abandoning BYOD and they justified their choice by saying that doing this will definitely ensure your organization's security.

Note: All the following qualitative survey questions are organized according to the Research Question that they correspond to.

RQ-1: What are the main differences between the traditional desktop-based approach and the BYOD approach according to the participants of the four selected sectors?

4.2.4 SQ-18: Describe your experience of shifting from the traditional approach to the BYOD approach.

For this survey question, we asked the respondents to share their experience of shifting from the traditional approach to the BYOD approach. The themes that emerged for SQ-18 for our four sectors are shown in the bar graph below: (see Fig. 4.9)

In this bar graph, "Code1" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-18. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:
The most dominant theme that emerged for SQ-18 for this sector was "Good" with a

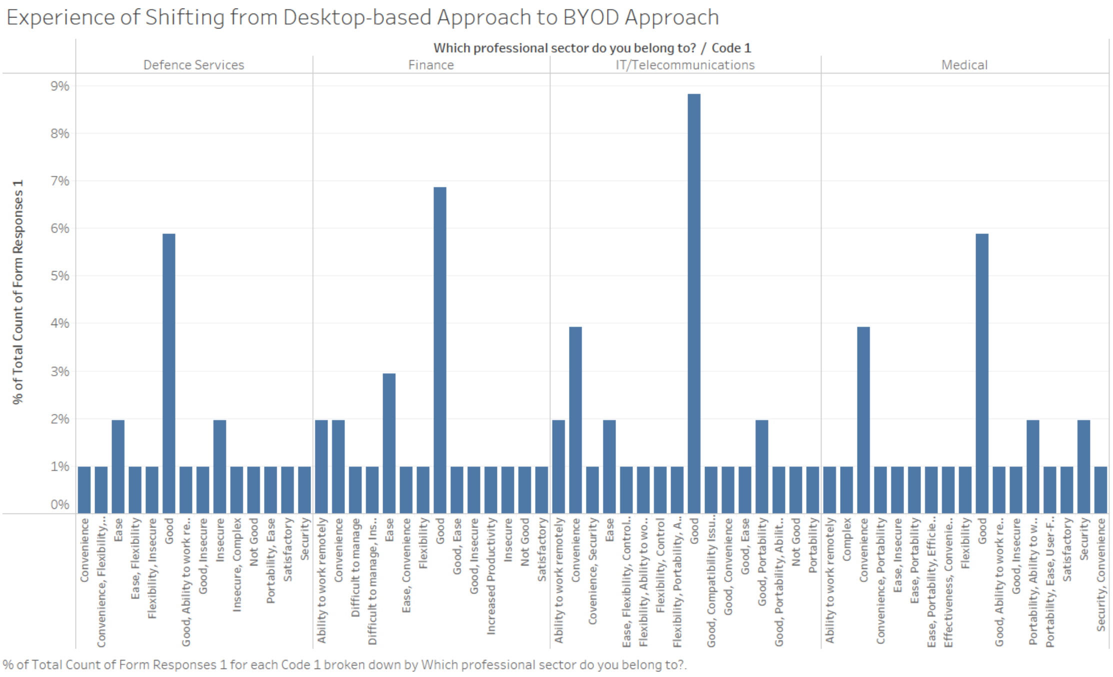


Figure 4.9: Experience of shifting from desktop-based approach to BYOD approach

percentage of **5.9%**. The participants were a little hesitant to express their experience in depth, but they did express their strong inclination towards the BYOD approach because of the numerous benefits that it offers. Apart from that, some participants considered BYOD to be more convenient, flexible, and a portable approach as compared to the traditional one. Some participants were also of the view that BYOD allows one to work remotely from wherever he or she is which eliminates the need of being physically present at the workplace all the time. However, some participants also considered BYOD to be complex to adopt while some of them were concerned about the security of this approach.

Finance:

The dominant theme for the Finance sector was also "Good" with a percentage of **6.9%**. However, for this sector, a handsome number of participants were also fascinated by the ease that the BYOD approach brings about. For them, this approach not only makes it all the more convenient to carry out their official tasks but it also allowed them to work more efficiently since they were quite familiar with the device they were using as it was owned by them.

IT/Telecommunications:

Again, for this particular sector, the dominant theme for SQ-18 was "Good" with a percentage of **8.9%**. However, the second most dominant theme for this sector was "Convenience" that is the participants thought that it is way more comfortable for them to work with their personally owned devices rather than working with organization owned devices that also had certain restrictions imposed on them.

Medical:

Just like the rest of the three sectors, the dominant theme for SQ-18 for the Medical sector was also "Good" with a percentage of **5.9%**. Moreover, just like the IT/Telecommunications sector, the second most dominant theme for the participants from the Medical sector was "Convenience". However, some participants of this sector also considered the personally owned devices to be more user-friendly that adds more to the convenience aspect of their usage at the workplace.

4.2.5 SQ-20: In your opinion, what are the differences between the traditional and BYOD approach?

For this survey question, we asked the respondents to share all the differences they could think of between the traditional and the BYOD approach. The themes that emerged for SQ-20 for our four sectors are shown in the bar graph below: (see Fig. 4.10)

In this bar graph, "Code3" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-20. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

For this particular sector, all the themes that emerged out for the question under discussion had the same percentages i.e. **1.7%**. Some of the participants from this sector considered the traditional approach to be secure but expensive whereas some of them believed that the organization owned devices offer a high rate of availability. There were still some of them who thought of the traditional approach to be insecure, however, they

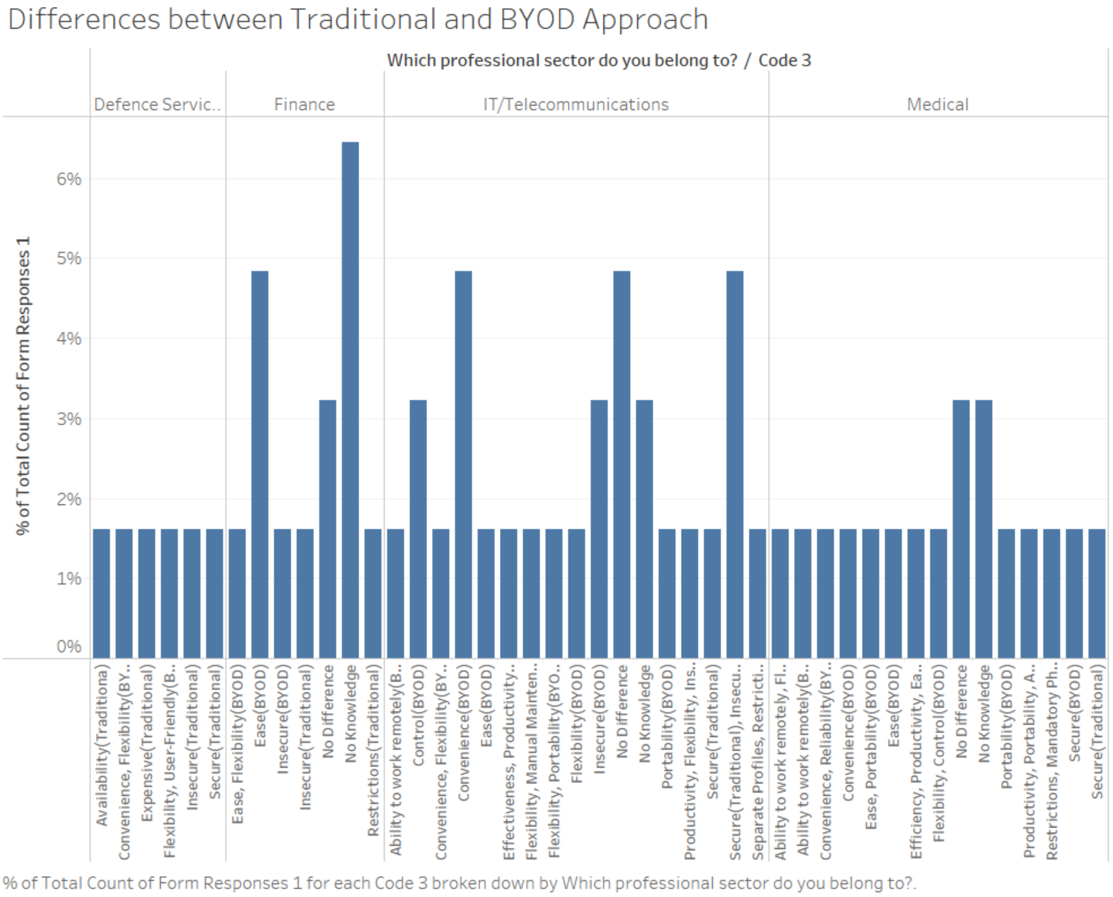


Figure 4.10: Difference between traditional and BYOD approach

did not mention the reason of saying so. Moreover, some of the participants considered the BYOD approach to be convenient, flexible, and user-friendly.

Finance:

The participants from the Finance sector came up with highly unexpected responses for this survey question as the responses of most of them fitted into the "No Knowledge" theme i.e. they could not comment on the differences between these two approaches because of their lack of knowledge about them.

IT/Telecommunications:

There were three most dominant themes that emerged for this sector for SQ-20 i.e. "Convenience (BYOD)", "No Difference", and "Secure (Traditional), Insecure (BYOD)" with the same percentages of **4.9%** each. It means that most of the participants from this sector considered BYOD to be more convenient as compared to the traditional approach. Some participants considered the traditional approach to be secure and the BYOD approach to be insecure since the organizations cannot employ their best security practices on the devices that are not owned by them. However, the "No Difference" theme was quite surprising for this sector but still, a good number of participants from this sector believed that there are no differences between the two approaches.

Medical:
For the Medical sector, two most dominant themes emerged for SQ-20 i.e. "No Difference" and "No Knowledge" with a percentage of **3.2%** each. Since the awareness of the participants from the Medical sector regarding BYOD was unreasonably low, therefore, both of these two themes can conveniently be attributed to their lack of knowledge.

4.2.6 SQ-24: What are the differences between the traditional and BYOD approach that give rise to the security issues?

For this survey question, we specifically asked the respondents to share those differences between the traditional and BYOD approach that were giving rise to the security issues. This question was also meant for those participants whose organizations had faced the BYOD security issues before. The themes that emerged for SQ-24 for our four sectors are shown in the bar graph below: (see Fig. 4.11)

In this bar graph, "Code7" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-24. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:
The most dominant theme for this sector was "Insecure (BYOD)" with a percentage of **30%**. It meant that the majority of the participants from the Defence Services believed that because the BYOD approach is insecure as compared to the traditional approach, therefore, facing the security issues while complying with the BYOD approach is not unusual. However, some of the participants also considered privilege escalation to be a

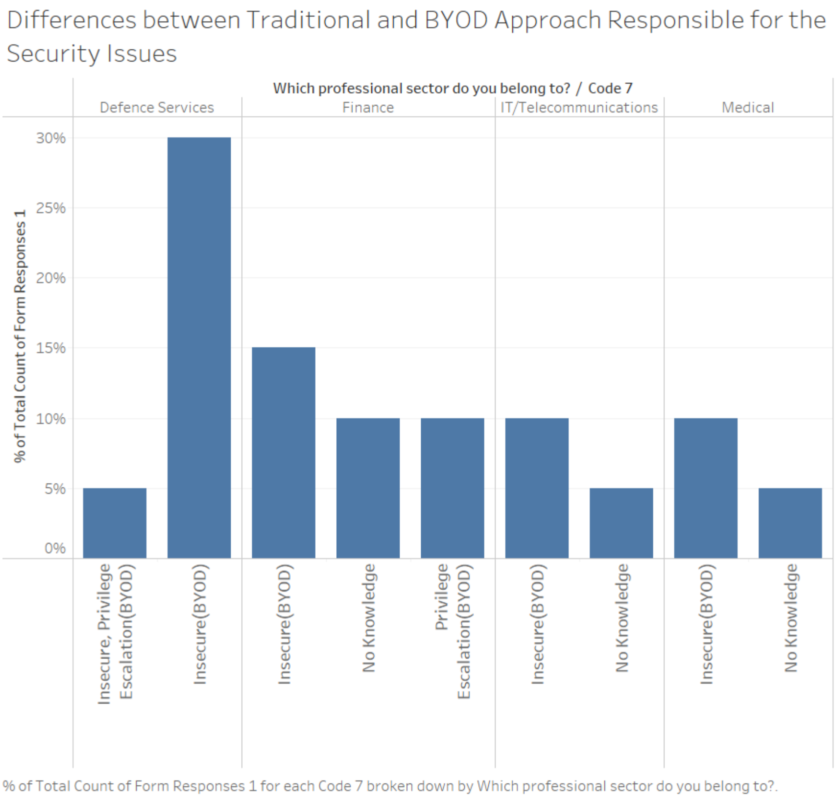


Figure 4.11: Differences between the traditional and BYOD approach responsible for the security issues

critical problem with the personal devices that can give rise to the security issues.

Finance:

The responses of the participants from the Finance sector also fitted dominantly in the "Insecure (BYOD)" theme with a percentage of **15%**. However, the other participants of this sector either did not have any knowledge about that or they also considered privilege escalation to be a major cause behind the BYOD security issues.

IT/Telecommunications:

Again, the dominant theme for this sector was also "Insecure (BYOD)" with a percentage of **10%** whereas some of the participants of this sector had no knowledge about this.

Medical:

The results for the Medical sector for SQ-24 were exactly the same as that of the IT/Telecommunications sector.

4.2.7 SQ-27: In your opinion, what are the differences between the traditional and BYOD approach? (for organizations who are not practicing BYOD currently)

For this survey question, we asked the respondents to share their opinions on the differences between the traditional and the BYOD approach. This question was meant for the participants whose organizations were not practicing BYOD currently. The themes that emerged for SQ-27 for our four sectors are shown in the bar graph below: (see Fig. 4.12)

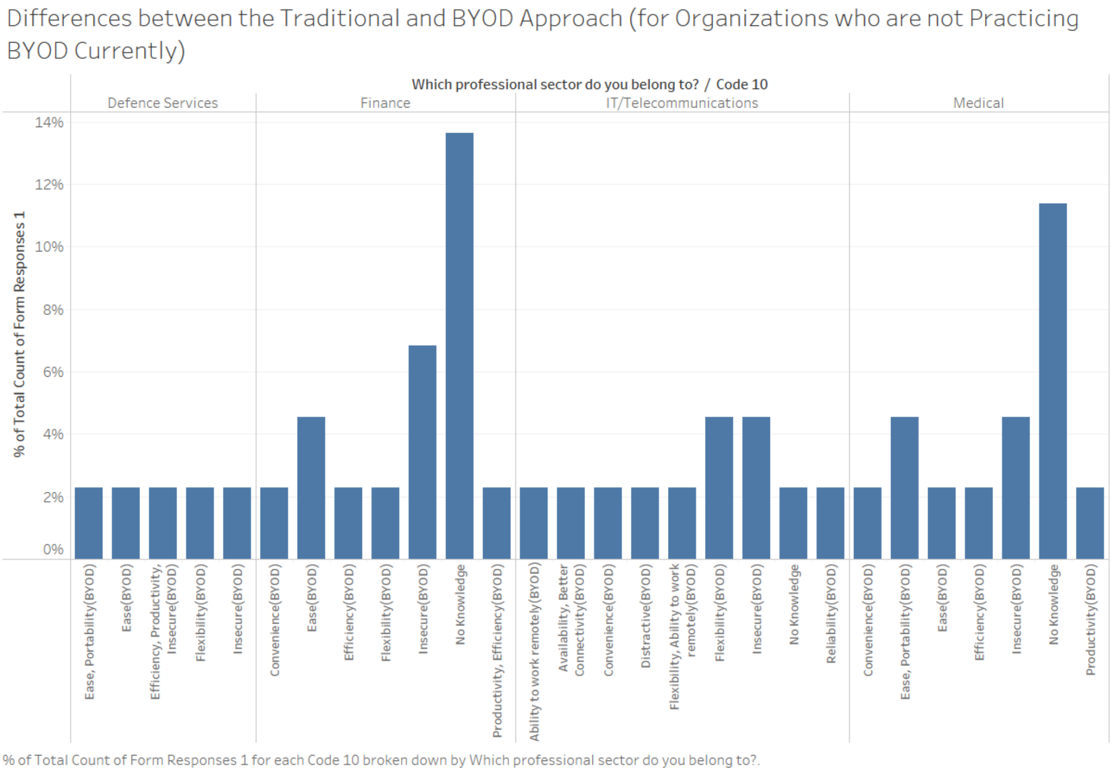


Figure 4.12: Differences between traditional and BYOD approach (for organizations who are not practicing BYOD currently)

In this bar graph, "Code10" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-27. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

All the themes that emerged for SQ-27 for this sector had equal percentages i.e. **2.2%**. Some of these participants considered the personal device usage as easy, portable, efficient, flexible, and productive whereas others thought of this approach to be insecure.

Finance:

The dominant theme for SQ-27 for this sector was "No Knowledge" with a percentage of **13.8%**. It meant that most of the participants were not much aware of the differences between the two approaches. Some also called BYOD as convenient whereas the other themes that emerged for this question for this sector were the same as that of the Defence Services.

IT/Telecommunications:

The two dominant themes that emerged for SQ-27 for this sector were "Flexibility (BYOD)" and "Insecure (BYOD)" with the percentages of **4.8%** each. The first theme referred to the wide range of devices to choose from as per an individual's convenience whereas the second theme referred to the security vulnerabilities of the BYOD approach. Apart from these, some of the participants considered BYOD to be an approach that provides better connectivity, 24/7 availability, reliability, and the one that can provide the ability to work remotely. However, there were still some participants from this sector who considered BYOD to be distracting because of the presence of a large number of non-work-related applications on the personal devices.

Medical:

The dominant theme for SQ-27 for this sector was "No Knowledge" with a percentage of **11.8%** which meant that the majority of the participants from this sector were not aware of the differences between these two approaches. However, the other themes that emerged for this sector with lesser percentages were the same as that of the Finance sector.

4.2.8 SQ-29: What are the differences between the traditional and BYOD approach that give rise to the security issues? (for organizations who are not practicing BYOD currently)

For this survey question, we asked the respondents to share the specific differences between the two approaches that give rise to the security issues. This question was also for the respondents belonging to the organizations who were not practicing BYOD currently. The themes that emerged for SQ-29 for our four sectors are shown in the bar graph below: (see Fig. 4.13)

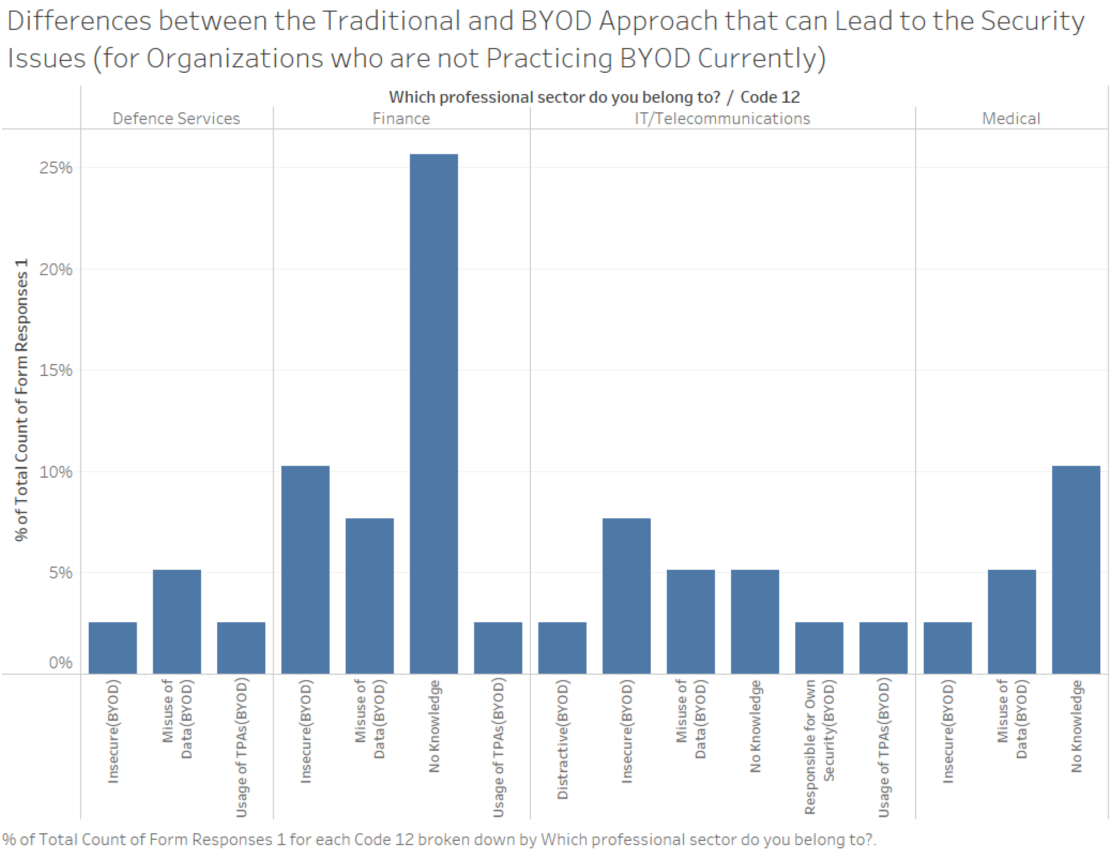


Figure 4.13: Differences between traditional and BYOD approach that can lead to the security issues (for organizations who are not practicing BYOD currently)

In this bar graph, "Code12" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-29. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The dominant theme for SQ-29 for this sector was "Misuse of Data (BYOD)" with a percentage of slightly more than **5%**. It meant that the ability of the employees to misuse the corporate data with the help of their personal devices can give rise to the BYOD security issues. Apart from this, some of the participants believed that the insecure nature of BYOD and usage of TPAs on the personal devices can also be responsible for the occurrence of BYOD security issues.

Finance:

The most dominant theme for this sector for SQ-29 was "No Knowledge" with a percentage of **25.4%** which meant that the majority of the participants from this sector had no knowledge about the question that was asked. The other themes with lesser percentages that emerged for this question were the same as that of the Defence Services.

IT/Telecommunications:

The most dominant theme for SQ-29 for this sector was "Insecure (BYOD)" with a percentage of **5.6%**. It meant that most of the participants from this sector believed that the insecure nature of the BYOD approach is responsible for causing the security issues. Some of the participants regarded BYOD to be distracting whereas some others believed that in the case of BYOD, one has to be responsible for his own security which can prove to be very challenging. The rest of the themes for this sector were the same as we have discussed for the Defence Services and the Finance sectors.

Medical:

The dominant theme for the Medical sector for SQ-29 was again "No Knowledge" with a percentage of **10.1%** which corresponds directly to the lack of knowledge of the professionals belonging to this sector regarding BYOD and its implementation. However, some participants of this sector were of the view that the insecure nature of BYOD and the misuse of data on personal devices can cause some major security issues.

RQ-2: What are the issues that arise as a result of shifting from the traditional approach to the BYOD approach?

4.2.9 SQ-22: Explain the BYOD security issue[s] in a few words (if your organization has faced any).

For this survey question, we asked the respondents to share the BYOD issue that their respective organization faced. This question was only meant for the respondents who had mentioned earlier in the survey that their organizations had faced security issues as a result of complying with the BYOD approach. The themes that emerged for SQ-22 for our four sectors are shown in the bar graph below: (see Fig. 4.14)

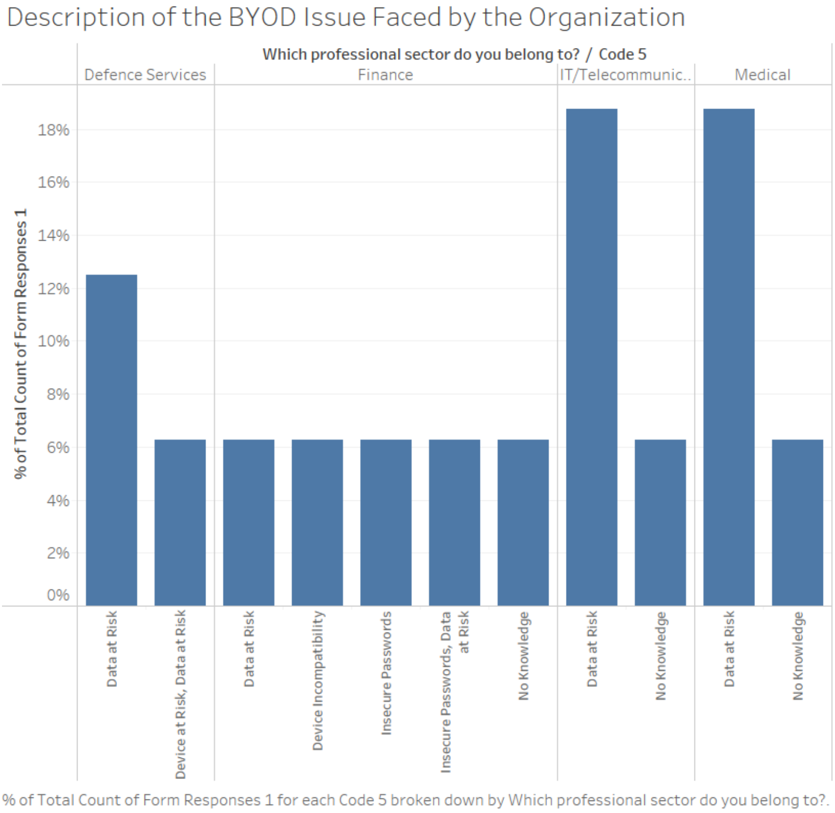


Figure 4.14: Description of the BYOD security issue faced by the organization

In this bar graph, "Code5" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-22. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The most dominant theme that emerged for this sector was "Data at Risk" with a percentage of **12.8%**. It meant that most of the participants from this sectors shared security issues that involved data breaches either because of privilege escalation, use of third party applications or even the employees intentionally sharing the corporate data with others.

However, some of the employees also gave such responses that fitted into the "Device at Risk" theme which meant that the personal devices are always vulnerable to theft or being lost or damaged as a result of which they can prove to be a potential threat to the organization's security.

Finance:

All the themes that emerged for this sector corresponding to SQ-22 had an equal percentage i.e. **6.2%**. Some of the respondents shared security issues revolving around the personal device's security or the data security. Some of them expressed concerns regarding device incompatibility which results in the BYOD devices becoming a loophole in the organization's security. Some participants believed that having insecure passwords for the personal devices can lead to some major security issues whereas others were not in a position to say anything in this regard since they had no knowledge about it.

IT/Telecommunications:

The dominant theme for this sector for SQ-22 was "Data at risk" with a percentage of **19%**. It means that the majority of the participants from this sector shared security issues that revolved around data theft, data misuse, data alteration, or data leakage.

Medical:

Same as the IT/Telecommunications sector, the dominant theme for the Medical sector was also "Data at Risk" with a percentage of **19%**.

4.2.10 SQ-28: What are the security issues that can possibly arise as a result of following the BYOD approach? (for organizations who are not practicing BYOD currently)

For this survey question, we asked the respondents to share their opinions on the security issues that can arise as a result of complying with the BYOD approach. This question was also for the participants belonging to the organizations who are not practicing BYOD currently. The themes that emerged for SQ-28 for our four sectors are shown in the bar graph below: (see Fig. 4.15)

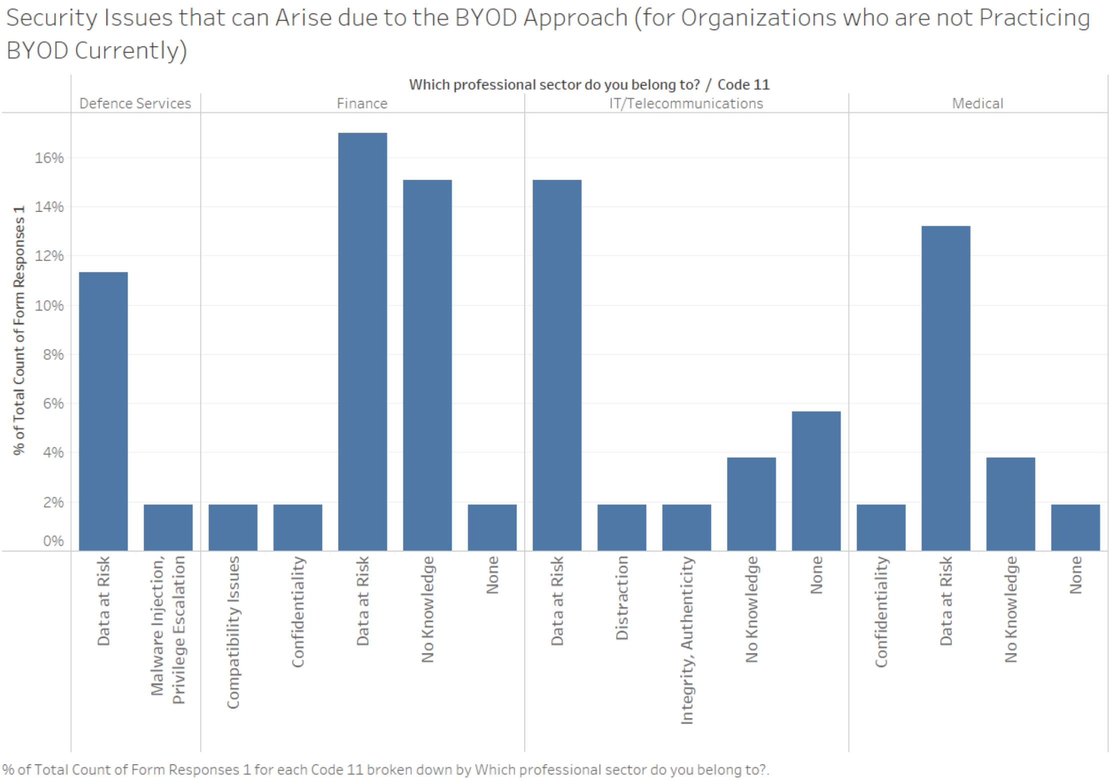


Figure 4.15: Security issues that can arise due to the BYOD approach (for organizations who are not practicing BYOD currently)

In this bar graph, "Code11" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-28. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

For this sector, the dominant theme was "Data at Risk" with a percentage of **11.6%**. It meant that in the opinion of these participants, the potential BYOD security issues will mainly revolve around data security. Other than that, some participants also considered malware injection and privilege escalation to be very important BYOD security issues.

Finance:
Again, for the Finance sector, the most dominant theme was "Data at Risk" with a percentage of **17%**. Apart from this, some participants also believed device compatibility and confidentiality to be the major BYOD security issues.

IT/Telecommunications:
The dominant theme for SQ-28 for this sector was also "Data at Risk" with a percentage of **15%**. Other than that, some participants from this sector also considered distraction, integrity, and authenticity as the potential BYOD security issues.

Medical:
Surprisingly, the dominant theme for SQ-28 for this sector was also "Data at Risk" with a percentage of **13.4%**. Other than that, some participants either did not have any knowledge about it or they considered confidentiality as a major BYOD security issue.

RQ-3: How are the organizations from the selected sectors tackling with these issues?

4.2.11 SQ-19: Explain the BYOD practices employed by your respective organization for avoiding the BYOD security issues.

For this survey question, we asked the respondents to share the BYOD practices that their organizations have implemented to avoid the security issues. The themes that emerged for SQ-19 for our four sectors are shown in the bar graph below: (see Fig. 4.16)

In this bar graph, "Code2" simply refers to the name of the column in which we have

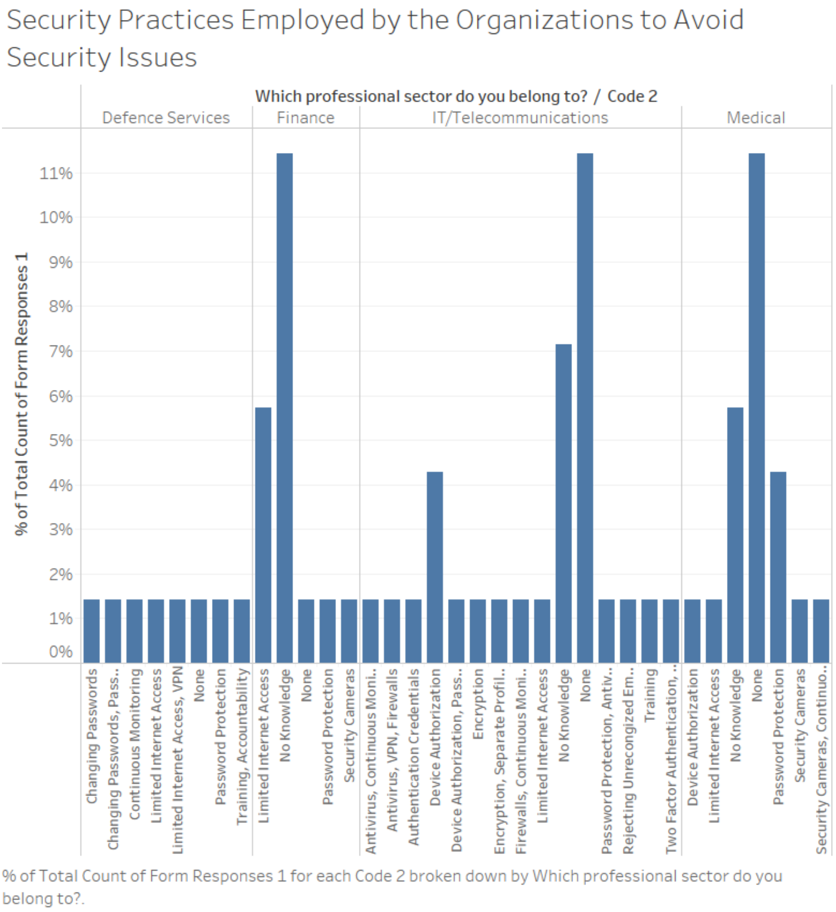


Figure 4.16: Security practices employed by organizations to avoid security issues

written the codes/themes corresponding to the responses of SQ-19. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

Surprisingly, all the different themes that emerged for SQ-19 for this sector had exactly the same percentages i.e. **1.5%**. It means that the numbers of participants who were in favour of these themes were equal. The themes that emerged for this question were "Changing Passwords" i.e. the employees shared that their respective organizations advise them to change their passwords frequently to avoid data leakage, "Password Protection" i.e. the employees were asked to keep their personal devices password protected all the time, "Continuous Monitoring" i.e. the organizations used to monitor the personal devices being used at the workplace continuously to avoid security breaches, "Limited Internet Access" i.e. the organizations did not allow the employees to connect their personally owned devices to insecure free Wi-Fi or even with any Wi-Fi dongles brought by the employees themselves, "VPN" i.e. virtual private networks should be used for organizational data communications, "Training" i.e. user training with respect to the correct BYOD usage is mandatory, "Accountability" i.e. proper check and balance should be maintained and their should be a proper mechanism to trace the person who is accountable for any potential BYOD security issue. Apart from these themes, some of the participants also gave such responses that fit into the "None" theme i.e. their respective organization had not employed any security practice to avoid the BYOD security issues.

Finance:
The most dominant theme for SQ-19 for this sector was "No Knowledge" with a percentage of **11.5%** which meant that most of the participants of the Finance sector were not aware of any security practices employed by their organizations to avoid the BYOD security issues. In other words, according to these participants, such security practices might exist but they had no knowledge about their existence since they considered it to be a highly technical matter.

IT/Telecommunications:
For the IT/Telecommunications sector, the most dominant theme for SQ-19 was "None" with a percentage of **11.5%** which was extremely shocking since it is a sector with a very technical background. This theme referred to the fact that the respective organizations have not employed any security practices for avoiding the BYOD security issues. Receiving such responses from the IT/Telecommunications sector is an extremely alarming situation.

Medical:
The respondents from the Medical sector were no different from that of the IT/Telecommunications sector in this regard i.e. their most dominant theme for SQ-19 was also "None" with a percentage of **11.5%**. Moreover, a handsome number of participants from this sector also went with the "No Knowledge" theme which corresponds to their lack of knowledge in this regard.

4.2.12 SQ-21: Suggest some possible improvements in the implementation of BYOD for strengthening its security.

For this survey question, we asked the respondents to suggest some improvements in the implementation of BYOD that can strengthen its security. The themes that emerged for SQ-21 for our four sectors are shown in the bar graph below: (see Fig. 4.17)

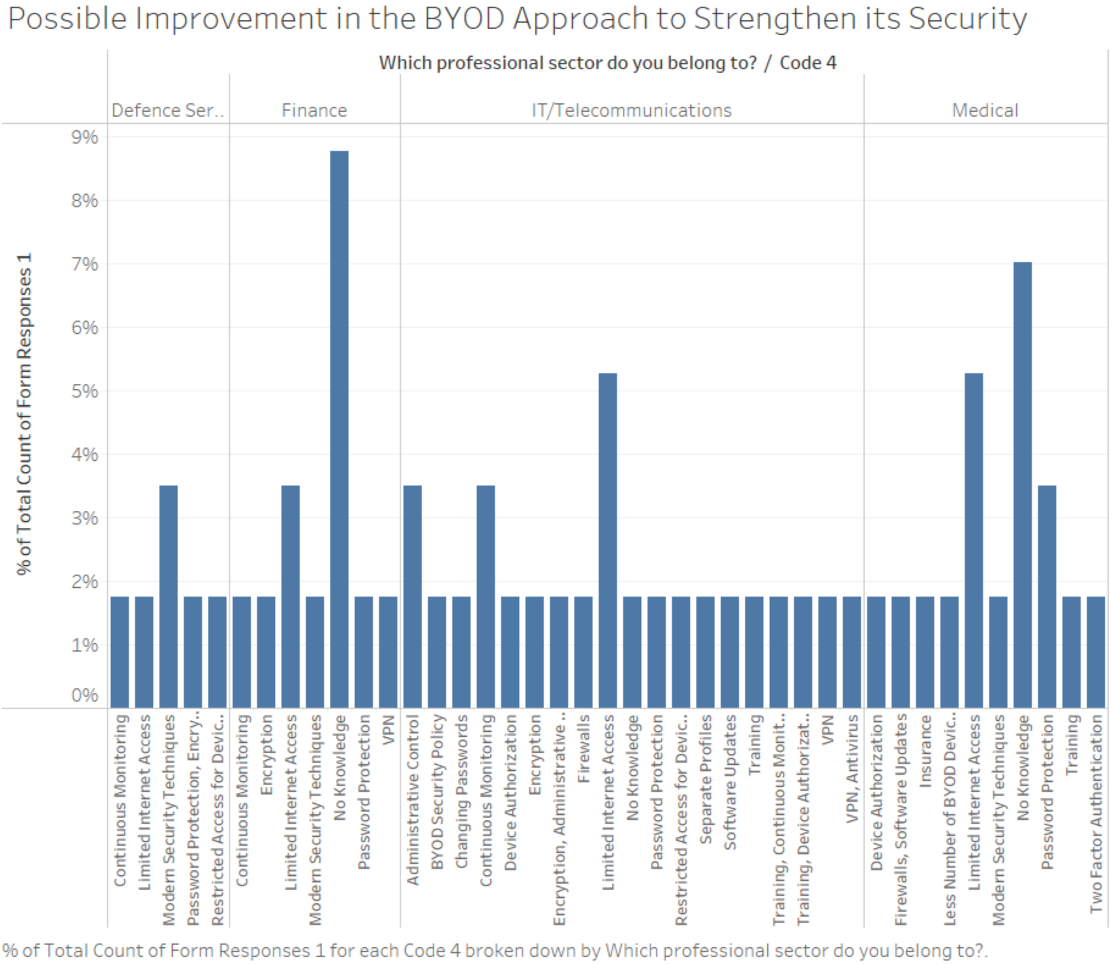


Figure 4.17: Possible improvement in BYOD approach to strengthen its security

In this bar graph, "Code4" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-21. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The most dominant theme that emerged for SQ-21 for this sector was "Modern Security Techniques" with a percentage of **3.5%**. All the participants whose responses fitted into this theme did not specifically mention any security practices as such rather they just used the "modern" terminology to express that their organizations need to be ahead in technology implementation to strengthen the BYOD security. Rest of the themes that emerged for this sector mainly revolved around password protection, use of encryption, continuous device monitoring, limiting the Internet access, and device authorization (registering the personal devices used within the workplace).

Finance:

For the Finance sector, the most dominant theme was "No Knowledge" with a percentage of **8.9%** which meant that they were not aware of any possible improvements in the implementation of BYOD. However, a good number of participants from this sector suggested limiting the Internet access to be a possible improvement in the direction of strengthening the BYOD security.

IT/Telecommunications:

The most dominant theme for this sector for SQ-21 was "Limited Internet Access" with a percentage of **5.2%** which referred to disallowing the BYOD devices to get connected to insecure free Wi-Fi. The second most dominant responses to this question for the IT/Telecommunications sector revolved around the themes of continuous monitoring and strengthening the administrative control or giving more authority to the organization's administration over the BYOD devices.

Medical:

For the Medical sector, the most dominant theme for this question was again "No Knowledge" with a percentage of **7%** which was not surprising for us since the professionals belonging to this sector are not aware of these technical details. However, a good number of the respondents from this sector still expressed that limiting the Internet access can prove to be a good improvement in this regard.

4.2.13 SQ-23: What was the strategy employed by your respective organization for tackling with the BYOD security issue[s]?

For this survey question, we asked the respondents to share strategies or the countermeasures that their respective organizations adopted to combat the BYOD security issues. Again, this survey question was solely meant for the respondents whose organizations have faced BYOD security issues. The themes that emerged for SQ-23 for our four sectors are shown in the bar graph below: (see Fig. 4.18)

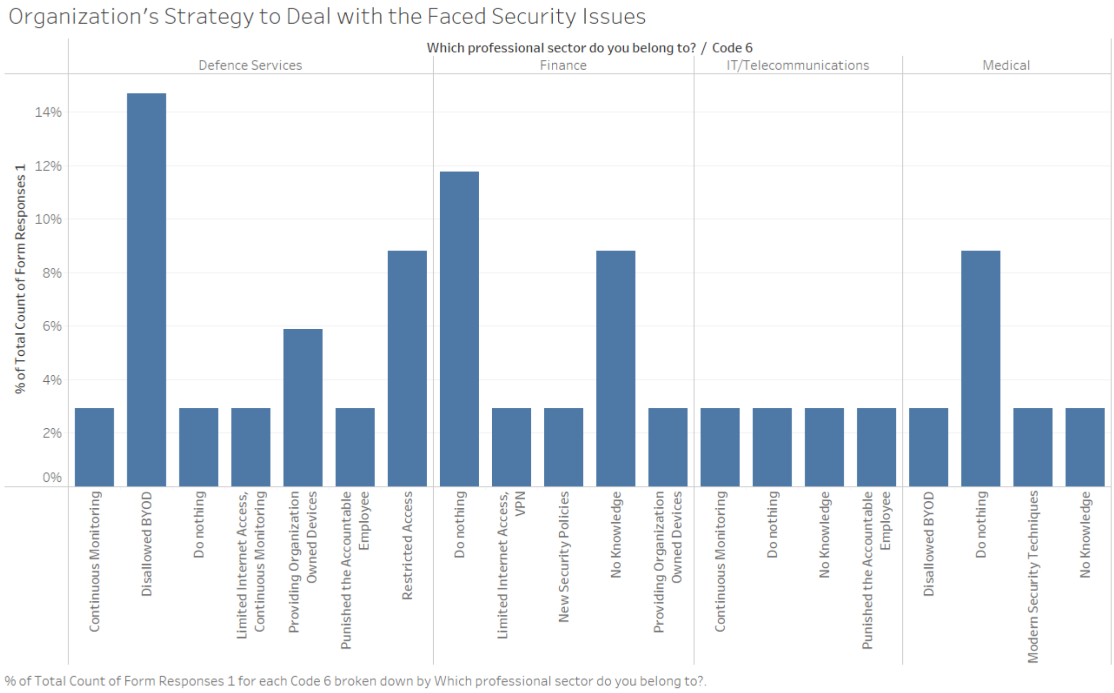


Figure 4.18: Organization's strategy to deal with the faced security issues

In this bar graph, "Code6" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-23. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The most common theme that emerged for SQ-23 for this sector was "Disallowed BYOD" with a percentage of **15%**. It meant that after facing the security issues as a result of complying with the BYOD approach, the organizations from this sector immediately abandoned the usage of personal devices at the workplace. Some participants shared that their organizations restricted the access of the personal devices after facing such issues whereas others started monitoring the personal devices more vigilantly after that.

Finance:

The most dominant theme for the Finance sector was "Do nothing" with a percentage of **11.8%**. It referred to the fact that most organizations belonging to this sector did nothing to tackle these security issues even after being a victim of them. This is quite a disconcerting situation since the Finance sector deals with highly critical data which must not be compromised so easily. Also, a good number of the participants from this sector did not have any knowledge about this.

IT/Telecommunications:

All the themes that emerged for this sector had an equal percentage i.e. **3%**. Some of the participants shared that their organizations started monitoring the personal devices continuously after facing the BYOD security issues while others expressed that employee or employees found accountable for such issues were specifically punished. However, some participants said that their organizations did nothing to deal with these issues whereas others did not have any knowledge about this.

Medical:

The most dominant theme for this sector for SQ-23 was "Do nothing" with a percentage of **9%**. It meant that most of the organizations belonging to this sector did nothing after facing the BYOD security issues. Some participants also shared that their organizations started employing modern security techniques whereas others said that their organizations banned the usage of personal devices at the workplace after facing such issues. However, still there were some participants who chose to stay silent in this regard because of their unawareness.

RQ-4: What are the BYOD security issues that still remain unattended within these organizations?

4.2.14 SQ-25: Which BYOD issues still remain unattended within your respective organization?

For this survey question, we asked the respondents to share all those BYOD security issues that still remain unattended. Again, this question was meant for those participants only whose organizations had faced BYOD security issues. The themes that emerged for SQ-25 for our four sectors are shown in the bar graph below: (see Fig. 4.19)

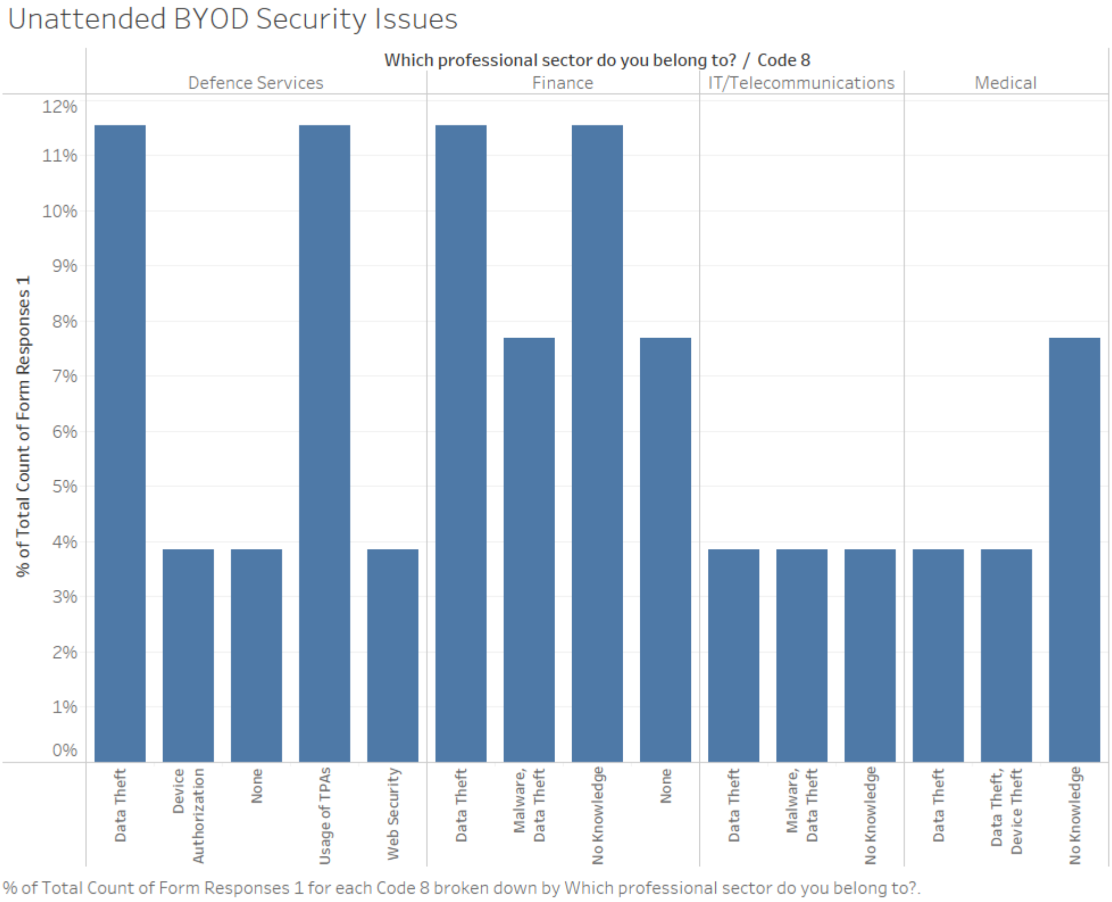


Figure 4.19: Unattended BYOD security issues

In this bar graph, "Code8" simply refers to the name of the column in which we have written the codes/themes corresponding to the responses of SQ-25. Moreover, we have also discussed these themes sector-wise in the following sections:

Defence Services:

The two most dominant themes that emerged for this sector for SQ-25 were "Data Theft" and "Usage of TPAs" with percentages of **11.5%** each. Data theft refers to the stealing of data by intruders or unauthorized users whereas usage of TPAs refers to the usage of third party applications on the employee owned devices. Apart from these dominant themes, some of the participants also believed that device authorization and web security are also some critical issues to deal with in this regard.

Finance:

The two most dominant themes for this sector were "Data Theft" and "No Knowledge" with percentages of **11.5%** each. It meant that the number of participants who expressed data theft as an unattended security issue in the Finance sector was equal to the number of participants who did not have any knowledge in this regard. Moreover, some participants also considered malware to be an unattended issue.

IT/Telecommunications:

The three themes that emerged for this sector for SQ-25 had equal percentages i.e. **3.9%**. Some participants from this sector considered data theft to be an unattended issue whereas others believed malware to be an unattended issue. However, there were also some participants who were not much aware about all this.

Medical:

The dominant theme for this sector for SQ-25 was "No Knowledge" with a percentage of **7.8%**. It meant that the participants belonging to the Medical background need to be more educated in this regard. However, some of the participants from this sector stated data theft and device theft as the unattended issues.

Chapter 5

Proposed BYOD Security Framework

After carrying out our survey and analysing our responses, we decided to propose a framework to all of our selected four sectors that they can implement within their respective organizations to avoid security issues while complying with the BYOD approach. In this regard, we did some initial research to study the existing frameworks and their scope. After that research, we decided to use an existing framework as a baseline and then proposing some improvements to enhance the effectiveness of that framework for our selected sectors.

5.1 Baseline Framework

After going through different BYOD security frameworks, we found [29] as the most appropriate and comprehensive framework for all the four sectors that we had selected. The basic model of this framework can be visualized from the image that follows (see Fig. 5.1). This model was a combination of different BYOD security frameworks from the previous literature, however, it was mainly based on the four domains of **COBIT 5**. These domains, in fact, formed the four stages of this framework. We will be taking a look at all of these stages in depth below:

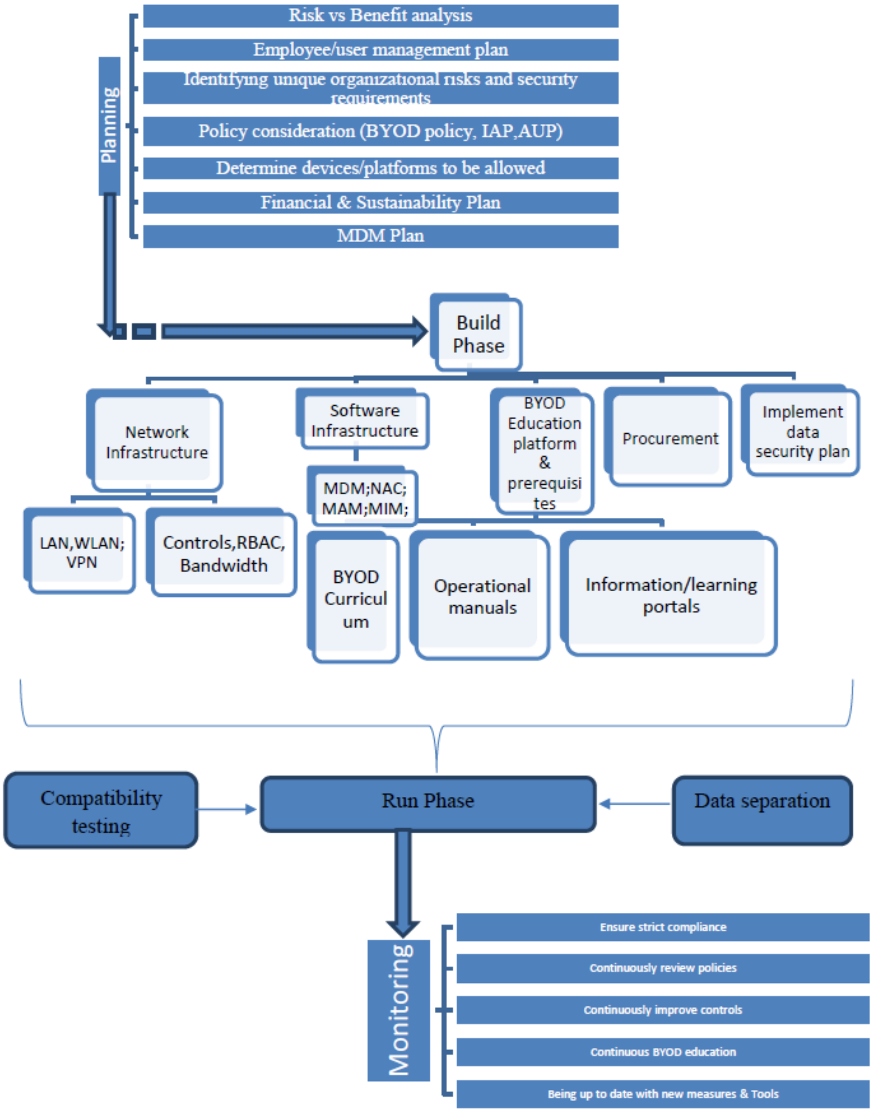

Planning
Risk vs Benefit analysis
Employee/user management plan
Identifying unique organizational risks and security requirements
Policy consideration (BYOD policy, IAP,AUP)
Determine devices/platforms to be allowed
Financial & Sustainability Plan
MDM Plan
Build Phase
Network Infrastructure
Software Infrastructure
BYOD Education platform & prerequisites
Procurement
Implement data security plan
MDM;NAC; MAM;MIM;
LAN,WLAN; VPN
Controls,RBAC, Bandwidth
BYOD Curriculum
Operational manuals
Information/learning portals
Compatibility testing
Run Phase
Data separation
Monitoring
Ensure strict compliance
Continuously review policies
Continuously improve controls
Continuous BYOD education
Being up to date with new measures & Tools

Figure 5.1: Model diagram of the baseline framework.

5.1.1 Planning

The **Planning** phase of this framework was a combination of multiple factors and we will state the purpose of each of them in detail over here. The **Risk vs Benefit Analysis** is mandatory in the planning phase because of the strong impact of users' perceptions in decision making. If the users perceive the risk of adopting a new technology to be overshadowing its benefits, then they will never go in the favor of that technology and vice-versa if the perceived risks are lower than the perceived benefits. That is why, a thorough analysis of the risks and benefits associated with the BYOD approach must be carried out before its adoption.

Once the employees are allowed to bring in their personal devices to the workplace, the next step is to device a proper **Employee/User Management** plan. The main goal of this plan is to identify the eligible candidates for the BYOD program and their registration so that the organization is well-aware of all the employees who are using their personal devices for organizational work. Every organization has a different set of values and a different culture altogether. That is why, in order to design an effective BYOD security framework, it is mandatory to **Identify the Unique Organizational Risks and Security Requirements** of an organization.

The **Policy Consideration** holds a crucial value in the planning phase because the policies lay the foundation stone of how the employees should act in any particular situation while especially highlighting all the permissible behaviors within an organizational premises. These policies should clearly highlight all the essentials of internet access and acceptable usage of personal devices as well as the applications residing within these devices. The next factor of the Planning stage is also related to this one and that is **Determining the Devices/Platforms to be Allowed**. Since we know that there is a large number of different devices available out there that come with different operating systems all of which may not be manageable for an organization. Therefore, it is always good to list down all the allowable devices and their respective platforms.

Then, there comes a **Financial and Sustainability Plan** which is put in place to figure out all the expenses that will be incurred while implementing the BYOD approach. Moreover, we also need to determine what additional resources would be required to facilitate this whole process such as adequate network bandwidth, essential human resources, and a sound IT infrastructure. Along with that, the business continuity, disaster recovery, and contingency plans should also be put into place. Finally, there comes a **Mobile Device Management (MDM) Plan** that should be there for a successful implementation of an MDM software. This software not only manages the personal devices but is also capable of controlling them. Therefore, its capabilities and their desired outcomes should be specifically listed down to avoid any issues in the future.

5.1.2 Build Phase

Just like the Planning phase, the **Build Phase** is also a combination of different factors. In this phase, all the planned resources are gathered and integrated so that they can work smoothly during the next phases. The first factor in the Build phase is to design the **Network Infrastructure** which includes implementing LAN, WLAN, VPN, etc. for ensuring secure network communication. Moreover, the organizations should also implement Role Based Access Control (RBAC) so that the employees are allowed to access only those organizational resources that are permitted to their respective role.

Then, there should be a proper **Software Infrastructure** so that the employees are not clueless about the fair usage of the personal devices at workplace. A good software infrastructure should comprise of Mobile Application Management (MAM), Mobile Information Management (MIM), Desktop Virtualization, and Network Access Control (NAC) tools. Apart from the technical controls, BYOD training and education is also very important for its successful implementation. For that, the **BYOD Education Platforms and Pre-Requisites** must also be laid down.

Then, there comes **Procurement** that refers to obtaining all the required resources once an organization has decided to use them for carrying out the planned activities. While procuring these resources, the procurement laws or policies must be kept in mind. Finally, the organizations should place their focus on the **Data Security** that will require a proper integration of all the security policies that were put into place during the Planning phase and the security software that will be employed to secure the personal devices used at the workplace.

5.1.3 Run Phase

The **Run Phase** as explained by [29] is a combination of the Planning and Build phases. When these two phases are combined and allowed to work together, only then the employees are allowed to start accessing the organizational resources with their personal devices. However, apart from the integration of the first two phases, the Run phase also checks the employees' devices for their compatibility and their eligibility for the BYOD program as stated by the Planning phase before actually granting them access to the organizational resources.

Moreover, the Run phase is also responsible for categorizing the data on a personal device into personal and organizational categories. This is done so that the IT administrators can easily implement the required security controls on the organizational data while setting the employees' personal data free from any such restrictions to as much extent as possible. This will also ensure the employees' privacy along with the organizational security. Lastly, it is also the job of a system administrator during the Run phase to ensure that the whole BYOD infrastructure is working as it was intended.

5.1.4 Monitoring

This is the last phase of our Baseline framework which is there to continuously assess the whole BYOD infrastructure and its working. This phase is essential because it not only highlights the shortcomings of the current framework but can also provide room for fixing them. Moreover, the Monitoring phase is, in fact, the one that allows you to bring in continuous improvements in your BYOD infrastructure to achieve best possible security while complying with the BYOD approach.

5.2 Shortcomings of the Baseline Framework

To test this Baseline framework, the researchers employed 7 participants from the ICT department of a government organization in Kenya. This framework was first explained to the selected participants after which they were presented with a survey containing 9 Likert Scale type questions. The summary of the responses of this validation survey can be seen from the chart below (see Fig. 5.2):

As you can see from this chart that the responses of the participants selected for the validation were highly in the favour of this framework, however, since the framework

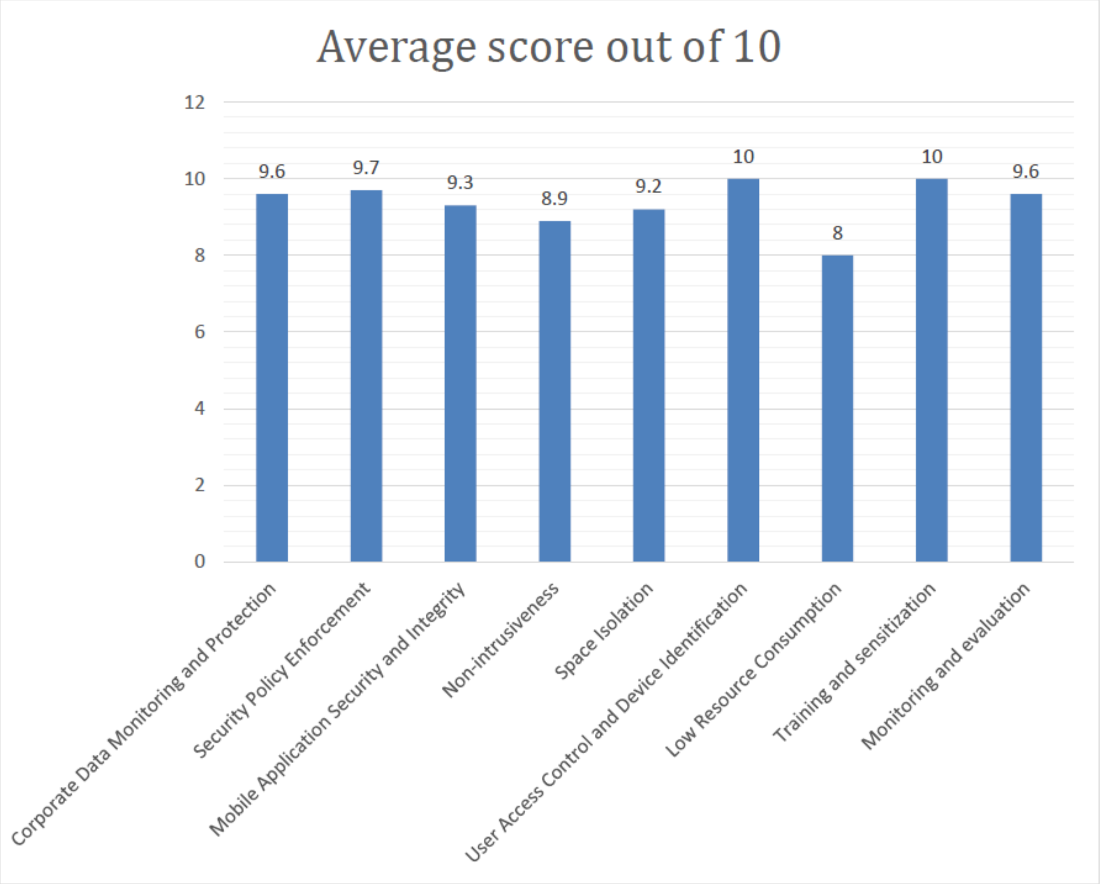


Figure 5.2: Average score out of 10 of the Baseline framework for different features.

was tested only with the professionals of a particular government organization in Kenya, therefore, there was still a chance that the perceptions of participants from other non-governmental sectors will be different about this framework. Therefore, after critically analyzing the different features of this framework, we decided to suggest improvements for the **three** least rated features of this framework i.e. **Non-Intrusiveness**, **Space Isolation**, and **Low Resource Consumption**. These improvements will be explained in the next section of this report.

After suggesting some possible improvements in the Baseline framework, we aimed to present it to a group of participants from our four selected sectors and test the effectiveness of this framework while especially focusing on the suggested improvements in the three least rated features. With this validation test, we wanted to figure out if there were any improvements in the scores for those features of this framework for the participants of our selected sectors in Pakistan or not.

5.3 Proposed Improvements in the Baseline Framework

Before proposing the improvements in the Baseline framework, we will show you the updated model diagram for our improved version of this framework (see Fig. 5.3):

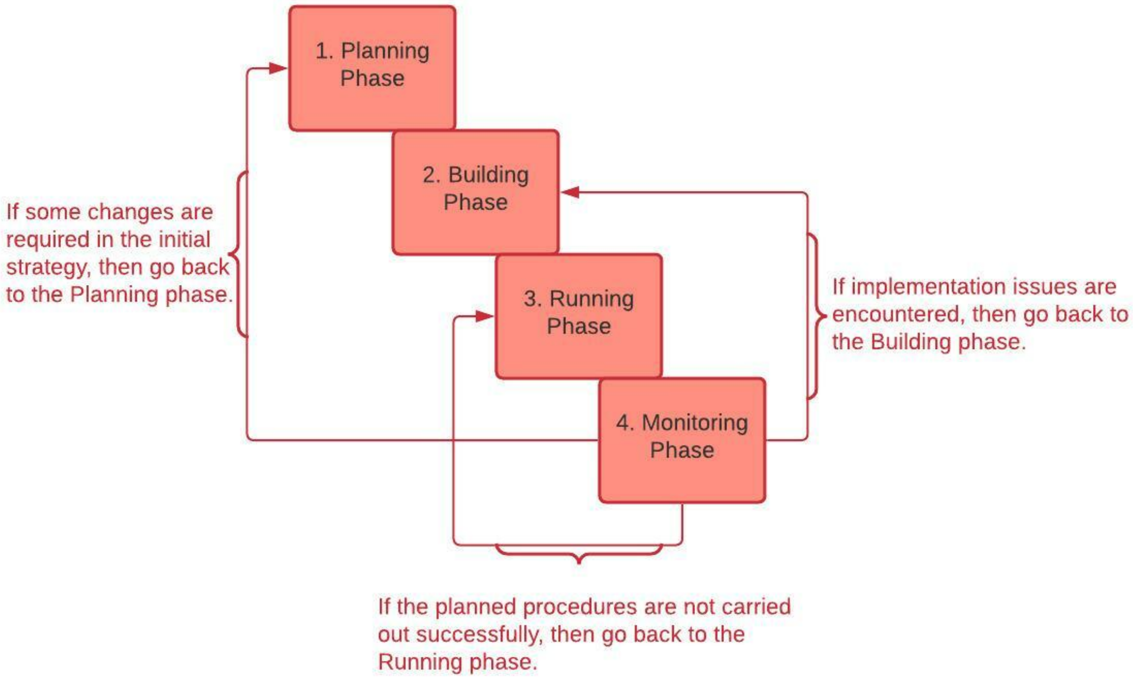

1. Planning Phase
2. Building Phase
3. Running Phase
4. Monitoring Phase
If some changes are required in the initial strategy, then go back to the Planning phase.
If implementation issues are encountered, then go back to the Building phase.
If the planned procedures are not carried out successfully, then go back to the Running phase.

Figure 5.3: Updated model diagram of the improved version of the Baseline framework.

First of all, we have made the Baseline framework iterative because there is always a room for improvement during all the stages of a process. If any issues are encountered while monitoring, then they can solely be fixed by going back to the respective stages which is possible only in an iterative framework. After doing that, we will be presenting to you the improvements for the three least rated features of the Baseline framework one by one.

5.3.1 Improvements for Non-Intrusiveness

For preventing intrusiveness, the strategies suggested in the Baseline framework were **Intrusion Detection Systems (IDS)**, **Network Access Control (NAC)**, and **Firewalls**. The first improvement that we would like to propose is that along with an IDS, an Intrusion Prevention System (IPS) must also be implemented within a BYOD environment. It is so because implementing an IDS is a monitoring strategy whereas implementing an IPS is a control strategy. In other words, with the help of an IDS, you can only detect that someone has broken into your network. Other than that, you cannot really do anything about it.

On the other hand, with the help of an IPS, you can actually prevent any malicious packets or an intruder from breaking into your system, hence, avoiding any intrusion from occurring in the first place. This will also offload a great burden from the IDS that was placed on it initially in the Baseline framework. Apart from that, instead of employing a simple Firewall, the organizations should consider going for the Next Generation Firewalls since they are capable of performing a deeper network inspection hence guaranteeing **Defense in Depth**.

5.3.2 Improvements for Space Isolation

The only strategy devised in the Baseline framework for space isolation was **Data Separation** which can mainly be implemented with the help of containerization. This technique creates separate profiles for the personal data and the organizational data on a BYOD device. However, there are a few concerns associated with this approach. Firstly, even after profiling, the notifications for the organizational applications are also visible within the personal profile that can potentially leak any organizational data to the personal profile.

Moreover, there are certain third party applications which when installed on the device require access permissions to all the data or applications residing on that device. This again has the potential to make the organizational data vulnerable. To prevent such things from happening, more emphasize should be paid on employee training and education regarding the usage and harms of the **Third Party Applications (TPAs)**. Only this kind of awareness can prevent the employees from installing such applications on the devices that they use at the workplace. This will ensure the safety and security of the critical organizational data residing within an employee's personal device.

Apart from that, the organizations should also ensure that there is least organizational data residing on an employee's personal device. It is mandatory so that the employees should only carry that organizational data within their personal devices which is absolutely necessary. In other words, the **Principle of Least Privileges** should be taken into consideration while allowing the employees to keep the organizational data within their personal devices. The lesser the amount of organizational data residing in an employee's personal device, the easier will it be to protect it from security breaches.

5.3.3 Improvements for Low Resource Consumption

The strategies suggested for low resource consumption in the Baseline framework were **Financial and Sustainability Plan** and **Network Infrastructure Plan**. If we try to dig deeply into these strategies, then the Baseline framework suggested that organizations should plan for all the additional resources that will be required for the successful implementation of the BYOD approach. Along with that, the fair usage of applications and devices should also be ensured with the help of **Role Based Access Control (RBAC)**.

However, based on the survey that we conducted for our research, most of the participants suggested restricting the usage of the **Social Media Applications** on the personal devices that are used at the workplace as a method of preventing BYOD security issues. Therefore, as an improvement for the low resource consumption, the organizations should consider placing restrictions on the usage of social media within the organizational premises. This will not only avoid the additional bandwidth consumption during the usage of such applications but will also prevent the employees from getting distracted from their work which was also a major concern with the usage of personal devices at the workplace highlighted by a majority of our surveyed participants.

5.4 Validation of the Improved Framework

In order to validate the Baseline framework after suggesting relevant improvements for its three least rated features, we followed the same approach which was adopted for the validation of the Baseline framework. First of all, we selected **3** participants from each of the four sectors at random (to avoid any biases) i.e. **12** participants altogether. We only made sure that the participants for this validation survey had already participated in our initial BYOD study. You can also take a look at the number of participants for this validation survey by going through the chart shown below (see Fig. 5.4):

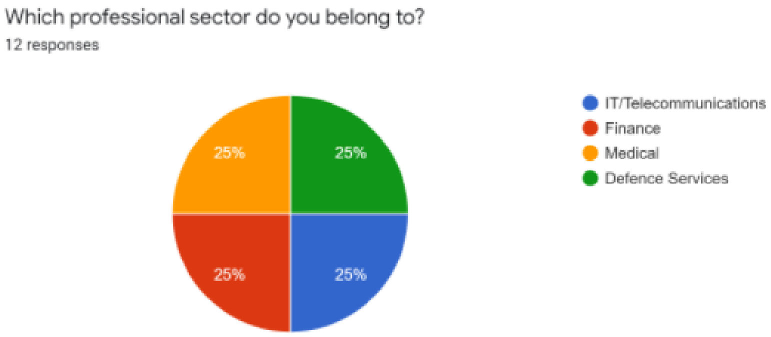


Figure 5.4: Sector-wise breakdown of the participants for the validation survey.

After selecting the target participants for the validation of the improved version of the Baseline framework, we explained this framework to them in detail while especially highlighting the proposed improvements and their potential advantages. Once the participants had a good knowledge of this framework, we shared with them our validation survey whose link is as follows: https://forms.gle/2Wxs3dVLo6dju5qW7.

This survey was mainly comprised of **9 Likert Scale** type questions in which we asked the participants to rate all the features of this framework on a scale of 1-10 where **1** represented **weak implementation** and **10** represented **strong implementation** of the said feature. In addition to that, we also asked the participants if they wished this framework to be employed within their respective organizations or not. The results of this validation survey for all the four sectors combined as well as individually will be discussed in the proceeding sections.

5.4.1 Combined Scores of all Four Sectors

First of all, we would like to discuss the combined ratings of all the four sectors for the main features of this framework to get a good overview. As far as the three features (for which we suggested improvements) i.e. **Non-Intrusiveness**, **Space Isolation**, and **Low Resource Consumption** are concerned, then the average scores out of 10 for these features were **9.5**, **9.5**, and **9.5** respectively (see Fig. 5.5) whereas in the original framework, these scores were **8.9**, **9.2**, and **8** respectively.

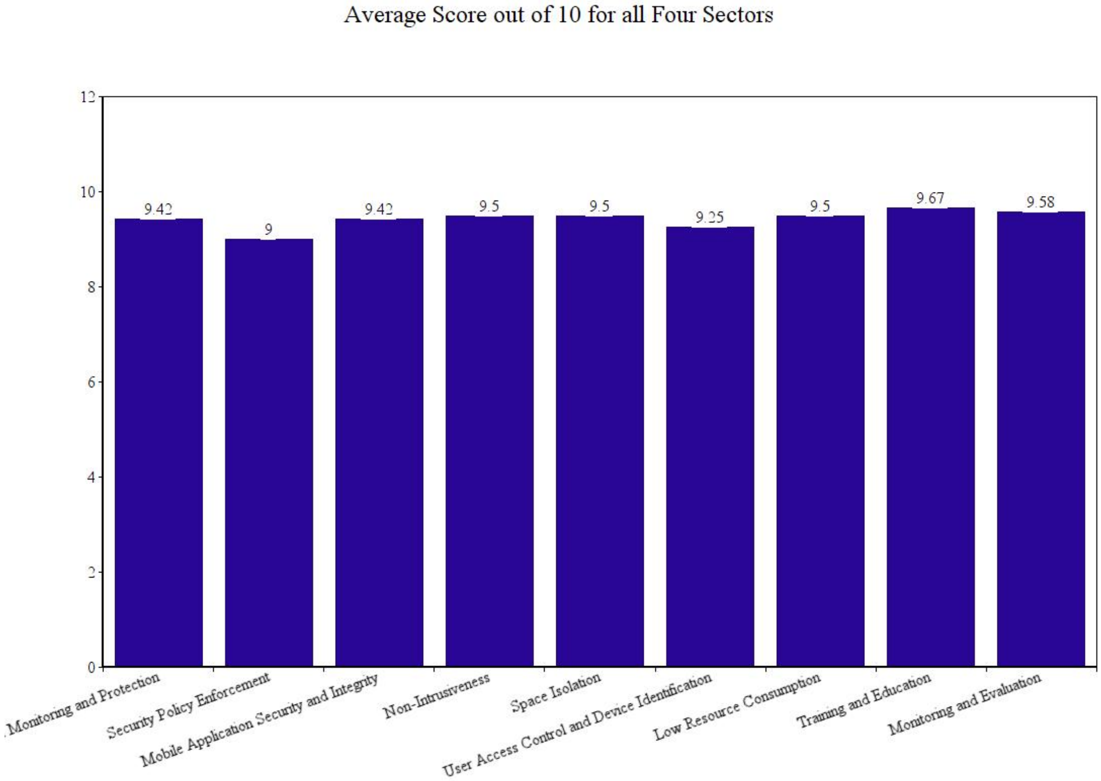


Figure 5.5: Average scores of the participants from all four sectors (combined) for the validation of the improved version of the baseline framework.

It means that the average scores for the three least rated features of the Baseline framework have significantly improved with our proposed modifications. However, as far as the other features of this framework are concerned, then their ratings were slightly lower than the actual framework which means that the participants from our four selected sectors either needed more clarification regarding those features or they required some additional modifications to those features too so that they can easily fit into their respective organizational environment. Now, we will discuss the sector-wise perceptions of the participants regarding the proposed improvements in the Baseline framework.

5.4.2 Scores of the Defence Services Sector

For the Defence Services sector, the average ratings of the three least rated features (after our proposed modifications) were **10**, **9.67**, and **9.33** respectively (see Fig. 5.6)

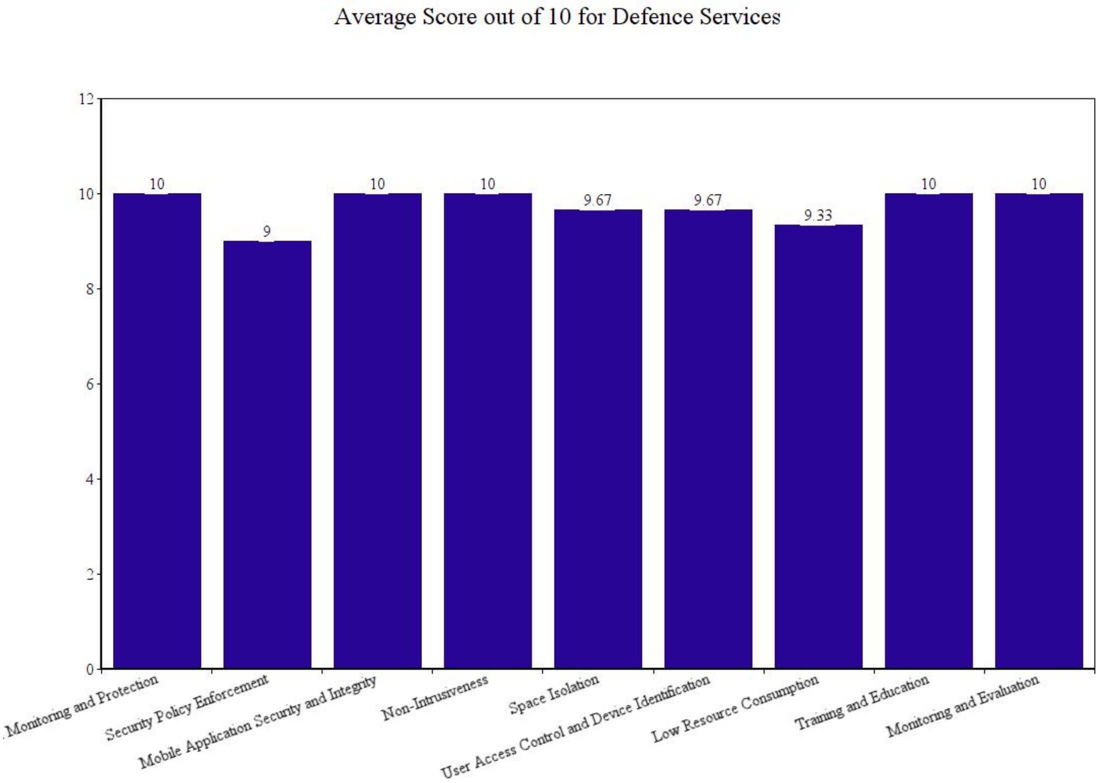


Figure 5.6: Average scores of the participants from the Defence Services sector for the validation of the improved version of the baseline framework.

which were again more than the ratings of the actual framework. It means that the participants from this sector for the validation survey were strongly in favor of our proposed improvements. However, for this particular sector, from the scores of the other features of this framework, we can infer that there is still some room for improvement for the **Security Policy Enforcement** feature of this framework.

5.4.3 Scores of the Finance Sector

The average ratings of the three least rated features (after our proposed modifications) for the Finance sector turned out to be **9.33**, **9.67**, and **9.67** respectively (see Fig. 5.7).

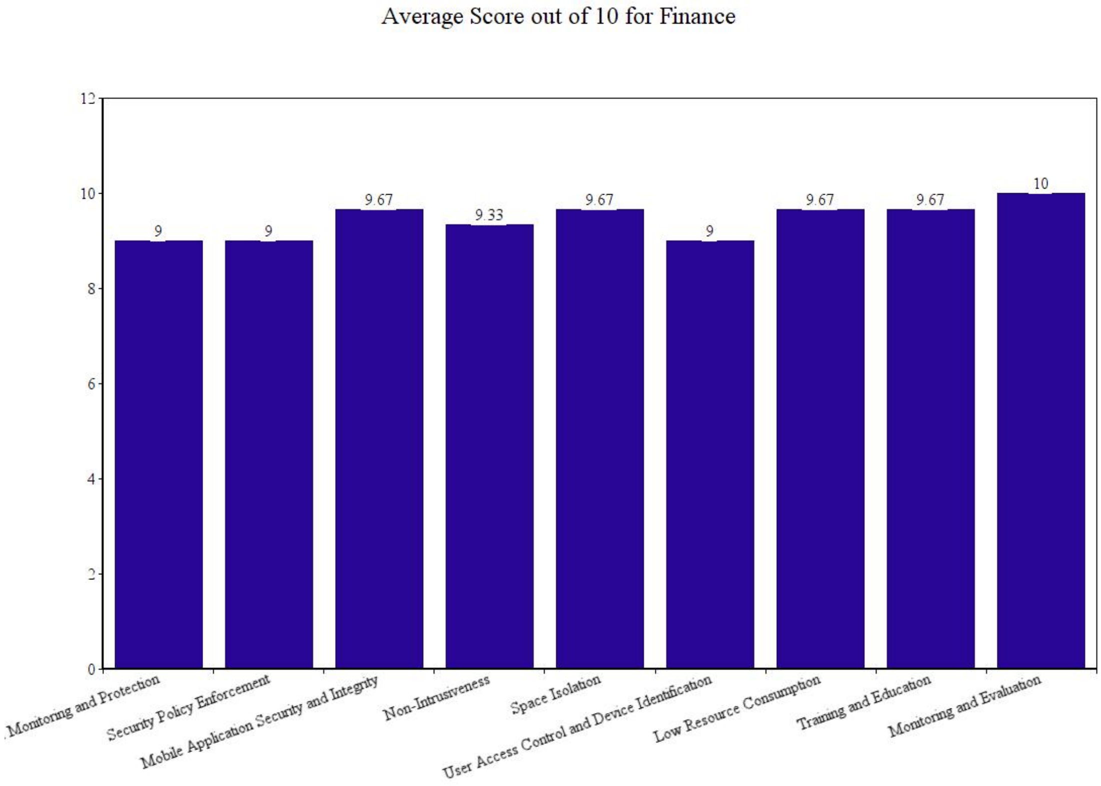


Figure 5.7: Average scores of the participants from the Finance sector for the validation of the improved version of the baseline framework.

Since these ratings were higher than the ones in the actual framework, hence we can say that the participants from this sector openly embraced our suggested improvements. However, for this particular sector, the features such as **Corporate Data Monitoring and Protection**, **Security Policy Enforcement**, and **User Access Control and Device Identification** can still be improved.

5.4.4 Scores of the IT/Telecommunications Sector

For the IT/Telecommunications sector, the average ratings of the three least rated features (after our proposed modifications) were **9**, **9.33**, and **9.67** respectively (see Fig. 5.8)

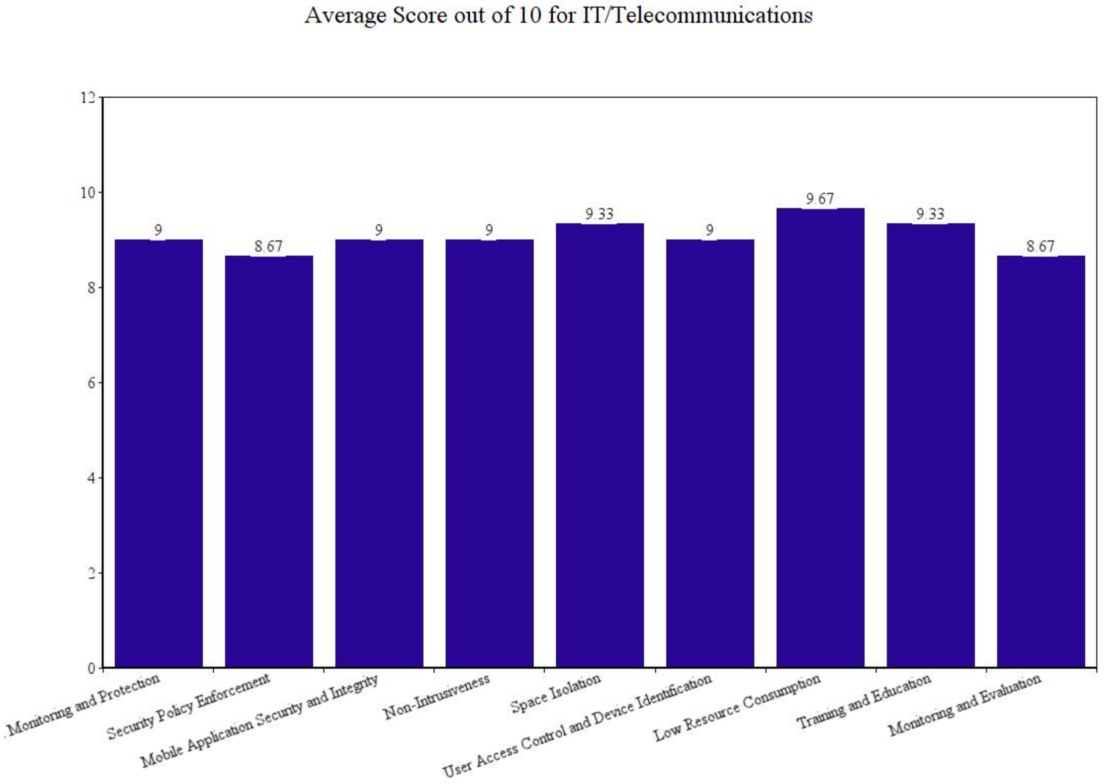


Figure 5.8: Average scores of the participants from the IT/Telecommunications sector for the validation of the improved version of the baseline framework.

which were again more than the ratings of the actual framework. It means that the participants from this sector for the validation survey supported our proposed improvements. However, for this particular sector, from the scores of the other features of this framework, we can conclude that there is still some room for improvement for the features such as **Security Policy Enforcement** and **Monitoring and Evaluation**.

5.4.5 Scores of the Medical Sector

The average ratings of the three least rated features (after our proposed modifications) for the Medical sector turned out to be **9.67**, **9.33**, and **9.33** respectively (see Fig. 5.9).

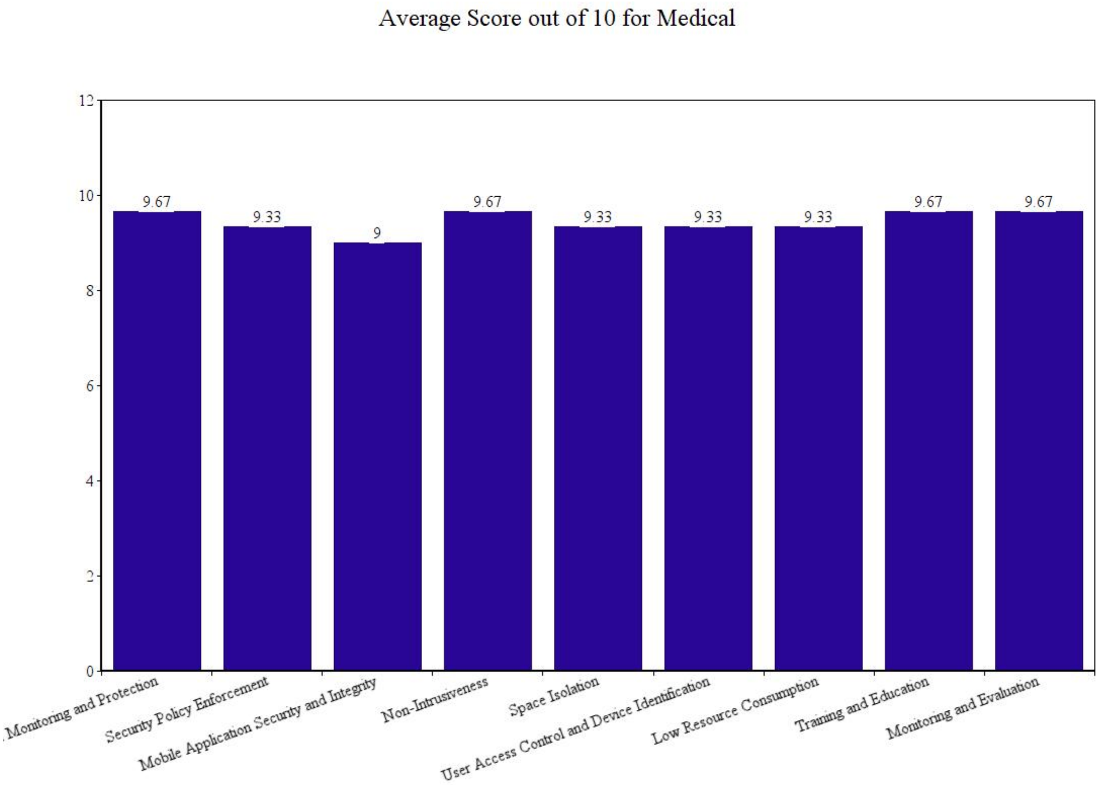


Figure 5.9: Average scores of the participants from the Medical sector for the validation of the improved version of the baseline framework.

Since these ratings were higher than the ones in the actual framework, hence we can say that the participants from this sector were very keen to adopt our suggested improvements. However, for this particular sector, the **Mobile Application Security and Integrity** feature can still be improved since the participants were highly concerned about the critical nature of the data that they deal with.

5.4.6 Acceptance of the Proposed Framework within all Four Sectors

With the results of the validation survey that we have already shared with you, you can easily realize that the participants from all the four sectors of our research i.e. **Defence Services**, **Finance**, **IT/Telecommunications**, and **Medical** welcomed our proposed improvements very warmly. However, to get their clear-cut verdict on the acceptance or rejection of the improved version of this framework, we asked the participants in our validation survey whether they want this framework to be implemented within their respective organizations or not.

To our surprise, all the **12** participants who were recruited for this validation survey wanted the improved version of this framework to be employed within their respective organizations (see Fig. 5.10).

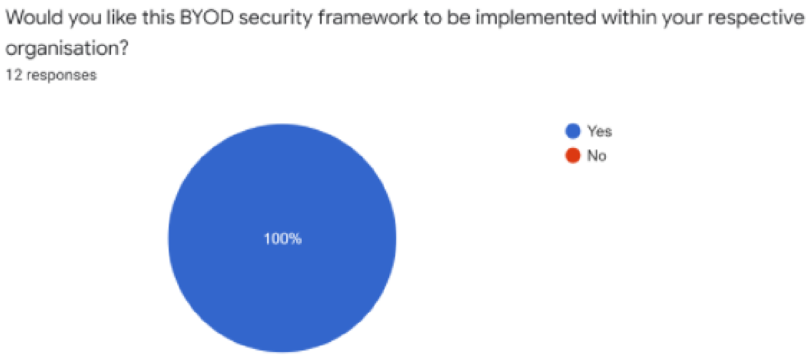


Figure 5.10: Acceptance rate of the improved version of the baseline framework in all four sectors (combined).

However, the varying ratings of the other features of this framework for each individual sector suggest the areas of further improvements for each particular sector according to their sector-specific needs. Overall, we can infer from the results of our validation survey that such a BYOD security framework is highly needed within all of our four selected sectors for a smooth implementation and running of the BYOD program.

Chapter 6

Recommendations, Conclusion, and Future Work

6.1 Recommendations

After carrying out this research, we are in a good position to give recommendations to the four sectors with whom we have performed our research on the basis of the observations we have made so far. In this section, first, we will be giving recommendations to all of our four selected sectors separately depending upon their BYOD security behaviors and practices followed by some general recommendations regardless of the sector.

6.1.1 Recommendations for the Defence Services Sector

For the Defence Services, the first thing that we would like to appreciate is that the overall security posture of this sector is far better than the rest of our three sectors. However, this still does not mean that there is no room for improvement in the security practices of this sector. With the help of the analysis of our collected data and its results, we have come up with the following recommendations for the Defence Services sector:

1. Instead of disallowing the BYOD practice altogether, special measures should be taken such as the deployment of MDM software so that even the professionals of

Defence Services can enjoy the benefits of the BYOD approach without compromising their critical data.

2. Special attention should be paid on to the enforcement of the BYOD policies within this sector.

3. The higher authorities should emphasize on the proper training of the employees regarding the correct usage of personal devices at the workplace.

4. Lastly, the employees should be made aware of the technical concepts such as privilege escalation, separation of profiles on the personal devices, etc. so that they can avoid the security issues as much as possible.

6.1.2 Recommendations for the Finance Sector

As far as the Finance sector is concerned, then we would like to rate its security posture as satisfactory. The reason behind saying this is that the participants from this sector who were well aware of the pros and cons of BYOD, were following good security practices, however, most of the participants from this sector had no knowledge about the technical details of BYOD because of which they were following poor security practices. The recommendations for the Finance sector are as follows:

1. Strong BYOD policies should be created after which the organizations of this sector can safely allow the usage of personal devices at the workplace.

2. After creating the BYOD security policies, their proper implementation should also be ensured.

3. Connecting the personal devices (especially the ones that are used at workplace) with insecure freely available Wi-Fi networks should be strictly avoided.

4. Even after adopting the BYOD approach within the organizations of this sector, the potential issues that can arise because of this approach must not be taken for granted.

5. The financial organizations should pay special attention on to the employees who are secretly using their personal devices at the workplace.

6. Protecting the personal devices with passwords alone cannot prevent the BYOD security issues rather the passwords should be strong enough to prevent password cracking.
7. Employees should be made well aware of the phishing attacks especially the ones that are carried out via emails.
8. Special attention should be paid on registering the personal devices that the employees intend to use at the workplace.
9. Employees from this sector should be educated about the benefits of using MDM software to manage the personal devices at the workplace effectively.

6.1.3 Recommendations for the IT/Telecommunications Sector

Since the professionals from the IT/Telecommunications sector belong to a highly technical background, therefore, we expected this sector to perform well in the research that we carried out. However, the results from this sector were quite surprising. There were some extremely insecure behaviors prevailing within the organizations of this sector because of which the employees of this sector were quite worried about the implications of using the personal devices at the workplace. The recommendations for the IT/Telecommunications sector are stated below:

1. Dedicated BYOD security policies should be created so that the personal devices can be used securely at the workplace.
2. If the BYOD practice is disallowed in an organization or BYOD security policies do not exist, then the employees should strictly avoid taking and using the personal devices at the workplace.
3. The employees from this sector should pay special attention on to encrypting the data residing in their personal devices and should never take this thing for granted.
4. Abandoning the BYOD approach is not the solution to avoid the security issues, therefore, this sector should work on implementing modern security controls along with BYOD security policies that can make the experience of using personal devices at the workplace safe and secure.

5. When the usage of personal devices is allowed at the workplace, the employees should be strictly prohibited to connect their devices with insecure free Wi-Fi networks.
6. The employees of this sector should be educated about the differences between the traditional and BYOD approach.
7. Special attention should be paid on tackling with the data theft and malware injection issues.

6.1.4 Recommendations for the Medical Sector

With our research, we managed to figure out that the Medical sector was the most ignorant about BYOD and its implementation details. Although, the personal devices were being used within the organizations belonging to this sector, however, the knowledge of the professionals belonging to this sector regarding all of our survey questions was almost negligible. Therefore, we have formulated the following recommendations for the Medical sector:

1. Strong BYOD policies should be created and implemented before allowing the employees to use their personal devices at the workplace.
2. Since this sector deals with highly critical healthcare data, therefore, if a particular organization belonging to this sector has disallowed the usage of personal devices at the workplace, then the employees must avoid doing so solely for the sake of their own ease and convenience.
3. The personal devices (especially the ones that are used at the workplace) must never be connected with insecure free Wi-Fi networks.
4. The implications of using the personal devices at the workplace must be clearly conveyed to the employees within this sector.
5. If only the senior employees of the healthcare organizations are allowed to use their personal devices at the workplace, then dedicated policies should be designed for them as well and their enforcement should also be carefully ensured.

6. If the employees of this sector are allowed to use their personal devices at the workplace only in their free time and that too for unofficial work, then those devices must not have any access to the corporate data.
7. The employees of this sector should be made aware of all the modern security practices so that they can conveniently opt to follow them without any reservations.
8. The employees of this sector should be properly educated on the differences of the traditional and the BYOD approach.
9. The employees of this sector should realize how important it is to deal gracefully with the security issues that arise because of using the personal devices at the workplace.
10. The BYOD security issues such as data theft and device theft should be given due consideration.
11. Employee training regarding the secure usage of personal devices at workplace is mandatory especially for the Medical sector.

6.1.5 General Recommendations

After talking about the sector-specific recommendations of our research, we would like to give some general recommendations as well regardless of the sector. This is done so that the industrial sectors other than the ones that we had selected for our research can also benefit from our findings and ensure the secure usage of personal devices at the workplace. The general recommendations extracted from the research that we carried out are as follows:

1. Before saying "No" to the BYOD approach, all the benefits that this approach offers must be taken into account. If the BYOD security risks for a particular organization overshadow these benefits, only then this practice should be prohibited.
2. The importance of BYOD security policies must be realized completely so that dedicated efforts should be put forth in this direction. Policy creation is one thing, however, its enforcement is even more crucial than that. Therefore, the higher authorities must ensure the enforcement of the designed policies.

3. Instead of abandoning the BYOD approach as a consequence of the security issues that arise because of it, the organizations should direct their efforts on designing such measures that can guarantee the best possible security while complying with this approach.

4. The deployment of a good MDM software can save an organization from a large number of potential security issues. Therefore, no compromise should be made in this regard especially if an organization is planning to adopt the BYOD approach.

5. Spreading the right kind of awareness regarding any particular technology or designing dedicated training programs should be made mandatory. This will prevent the employees of an organization from making careless mistakes (which will later on become security loopholes) because of their negligence or lack of knowledge about a technology.

6. Employees should especially be educated about the most common security controls such as **Confidentiality**, **Integrity**, **Availability**, **Authentication**, **Authorization**, and **Non-Repudiation**. They should realize the significance of each of these controls so that they are able to make wise security decisions.

7. One of the major security challenges with BYOD is the use of TPAs on the personal devices. The unnecessary usage of such applications should either be banned on the personal devices used at the workplace or it should be restricted in such a way that they cannot cause any harm to the corporate data. Moreover, doing this will also help in preventing the distraction that is caused by the personal device usage at the workplace.

8. Even if an organization is granting the access of the corporate data to the personal devices of the employees, that data should not be allowed to be downloaded on the personal device in any situation. Doing this will not only prevent the deliberate but also the unintentional leakage of the data.

9. None of the personal devices should be given more privileges than they need. In other words, the organizations must ensure that the personal devices being used within the workplace perfectly comply with the **Principle of Least Privileges**.

10. According to our research, since the most commonly used personal device at the

workplace is **Mobile Phone**, therefore, the future security solutions must focus on the security of this device more than any other out there.

11. The employees should realize that using the **Social Networking Applications** at the workplace can cause some major security setbacks to their organizations. Therefore, they should avoid doing this to as much extent as possible.

12. According to our research, most of the participants were of the view that the security controls that revolve around **Confidentiality** are the most important for protecting the data on their personal devices. This opinion might just be there because of the common use of this terminology in their daily lives. Therefore, they should be well aware of the importance of the other security controls too. Only then, they will be able to pick out the most important security controls according to their respective needs since no single security control can guarantee **100%** security.

13. Organizations should pay special attention on the fact that the policy that they have designed might not be understandable for their employees. Therefore, either it should be designed in such a way that it gets self-explanatory or the organizations should make sure to convey it to their employees properly.

14. The practice of creating strong passwords and using two factor authentication should be given due importance. Doing this can prevent some of the most commonly occurring security issues.

15. Lastly, the employees as well as the organizations should understand that **100%** security or **perfect** security is just a myth. There is always a trade-off between **security** and **usability**. Therefore, while trying to make our data or devices secure, we must not compromise their usability. Otherwise, we will eventually render them useless.

6.2 Conclusion

With this research, our aim was to know the current state of BYOD in our four selected sectors i.e. **Defence Services**, **Finance**, **IT/Telecommunications**, and **Medical**.

We wanted to explore how far the BYOD practice has penetrated within the organizations belonging to these sectors and to what extent the employees of these organizations are comfortable with using their personal devices at their respective workplaces. In this quest, we managed to unravel many interesting findings regarding the BYOD implementation within these four sectors.

We came to know that quite a large number of employees of these sectors were in the favor of using personal devices at the workplace because of the ease and convenience that they offer. However, some of the organizations within these sectors were still hesitant to adopt this approach because of its security vulnerabilities. Such organizations were discouraging this practice completely rather than working on the countermeasures of tackling with the security issues. However, even within these organizations, some employees were secretly using their personal devices within the organizational premises without bringing it in the knowledge of the higher authorities.

If we draw a comparison between the security practices of our four selected sectors, then in terms of the awareness of BYOD and the related security issues, the Defence Services sector was far better than the rest of the three. The security practices of the IT/Telecommunications and the Finance sectors were more or less the same. However, the most ignorant sector in this regard was the Medical sector since the professionals belonging to this sector were not even aware of the basics of the BYOD paradigm. Despite that, they were still using their personal devices at the workplace.

As far as the technicalities of our research are concerned, then we chose to make use of both the qualitative and the quantitative research approaches. The former one was used to get an in-depth knowledge of the perspectives of our participants whereas the latter one was used to get concrete statistics upon which the future researches can be based. All the facts and figures shared in this research have been collected through a real research conducted with the four industrial sectors of Pakistan.

If we talk about the contribution of our research work, then there were no previous studies carried out in Pakistan especially in this domain. The policy making guidelines were there but again, they were not tested with real-user feedback because of which following those guidelines as it is was a subject of serious concern for most of the organizations. Now, when a real research has been carried out within these four sectors, it will no longer be difficult to have a sound implementation of BYOD within these sectors at least. Therefore, our research laid the foundation stone in the domain of exploring BYOD and all of its pros and cons that one can face as a result of complying with this approach in Pakistan.

6.3 Future Work

The sole data collection method for this research was **Online Survey**. Although, in the beginning, we intended to carry out some interviews too but because of the COVID-19 pandemic, the in-person interviews were obviously not possible. As far as the online interviews are concerned, then because of the critical nature of most of our selected sectors, none of the employees from these sectors were willing to participate in the online interviews. Therefore, future researches may focus on collecting data through the interviews (if possible) to gain more clarity regarding the opinions of the participants since most of the participants do not open up much in the online surveys.

As far as the Defence Services sector is concerned, then the participants of that sector were quite hesitant to share their true opinions regarding our survey questions because of which we had to rely only on the limited information that they provided. This is also the reason behind the less number of responses that we managed to collect from this sector. In the future, the researchers might first make an attempt to convey the scope of their research effectively to this particular sector so that more participation from this sector in the future researches can be expected. Since a single security solution cannot cater to all the security requirements, therefore, the proposed framework in this research should be customized specifically to meet the needs of each of our four sectors so that at least these four sectors can conveniently embrace the BYOD approach.

The general security policy making guidelines of the organizations should also be refined (if needed) in the light of the findings of this research. Moreover, other industrial sectors of Pakistan should also be investigated with respect to their BYOD adoption and the respective security issues that they face. By carrying out such researches more often, we will be able to make the organizations realize that abandoning a technology solely because of its potential security issues is never a wise choice rather the approach of taking the relevant measures to avoid those issues and enjoying the benefits of that technology should be adopted. In the end, we would just like to say that technology is an innovation between good and evil. Now it is up to us whether we use it to build or to destroy.

References

[1] Kathleen Downer and Maumita Bhattacharya. Byod security: A new business challenge. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, pages 1128–1133. IEEE, 2015.

[2] Kevin Timms. Byod must be met with a wider appreciation of the cyber-security threat. *Computer Fraud & Security*, 2017(7):5–8, 2017.

[3] Manmeet Mahinderjit Singh, Chen Wai Chan, and Zakiah Zulkefli. Security and privacy risks awareness for bring your own device (byod) paradigm. *International Journal of Advanced Computer Science and Applications*, 8(2):53–62, 2017.

[4] Abubakar Garba Bello, David Murray, and Jocelyn Armarego. A systematic approach to investigating how information security and privacy can be achieved in byod environments. *Information & Computer Security*, 2017.

[5] Alex Koohang, Maria Teresa Riggio, Joanna Paliszkiewicz, and Jeretta Horn Nord. Security policies and data protection of mobile devices in the workplace. *Issues in Information Systems*, 18(1), 2017.

[6] Daniel Petrov and Taieb Znati. Context-aware deep learning-driven framework for mitigation of security risks in byod-enabled environments. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pages 166–175. IEEE, 2018.

[7] Nazaraf Shah, Arun Shankarappa, et al. Intelligent risk management framework for byod. In *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, pages 289–293. IEEE, 2018.

[8] Lixuan Zhang Zhang, Matthew Mouritsen, and Jeffrey R Miller. Role of perceived

value in acceptance of “bring your own device” policy. *Journal of Organizational and End User Computing (JOEUC)*, 31(2):65–82, 2019.

[9] Cindy Zhiling Tu, Joni Adkins, and Gary Yu Zhao. Complying with byod security policies: A moderation model based on protection motivation theory. *Journal of the Midwest Association for Information Systems (JMWAIS)*, 1:11–28, 2019.

[10] Xue Yang, Xinwei Wang, Wei Thoo Yue, Choon Ling Sia, and Xin Luo. Security policy opt-in decisions in bring-your-own-device (byod)–a persuasion and cognitive elaboration perspective. *Journal of Organizational Computing and Electronic Commerce*, 29(4):274–293, 2019.

[11] Hao Chen, Ying Li, Lirong Chen, and Jin Yin. Understanding employees’ adoption of the bring-your-own-device (byod): the roles of information security–related conflict and fatigue. *Journal of Enterprise Information Management*, 2020.

[12] Madhavi Dhingra. Legal issues in secure implementation of bring your own device (byod). *Procedia Computer Science*, 78:179–184, 2016.

[13] Andrea Vaca Herrera, Mario Ron, and Carlos Rabadão. National cyber-security policies oriented to byod (bring your own device): Systematic review. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–4. IEEE, 2017.

[14] T Pereira, L Barreto, and A Amaral. Network and information security challenges within industry 4.0 paradigm. *Procedia manufacturing*, 13:1253–1260, 2017.

[15] Musa Abubakar Muhammad, Aladdin Ayesh, and Pooneh Bagheri Zadeh. Developing an intelligent filtering technique for bring your own device network access control. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, pages 1–8, 2017.

[16] Musa Abubakar Muhammad, PB Zadeh, and Aladdin Ayesh. Improving security in bring your own device (byod) environment by controlling access. ACM, 2017.

[17] Melva M Ratchford and Yong Wang. Byod-insure: A security assessment model for enterprise byod. In *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, pages 1–10. IEEE, 2019.

[18] Fenio Annansingh. Bring your own device to work: How serious is the risk? *Journal of Business Strategy*, 2020.

[19] Marzie Astani, Kathy Ready, and Mussie Tessema. Byod issues and strategies in organizations. *Issues in Information Systems*, 14(2), 2013.

[20] Mohd Yusri Jusoh, Haryani Haron, and Jasber Kaur. Byod practices in malaysia public sector. 2016.

[21] Saima Nisar and Wan Rozaini Sheik Osman. Factors affecting the intention to adopt byod among healthcare professionals in pakistan. 2016.

[22] Tafheem Ahmad Wani, Antonette Mendoza, and Kathleen Gray. Byod in hospitals-security issues and mitigation strategies. In *Proceedings of the Australasian Computer Science Week Multiconference*, pages 1–10, 2019.

[23] Chalee Vorakulpipat, Chantri Polprasert, and Siwaruk Siwamogsatham. Managing mobile device security in critical infrastructure sectors. In *Proceedings of the 7th International Conference on Security of Information and Networks*, pages 65–68, 2014.

[24] Scott Thomas Migdalski. Investigating military instructors' experiences with students' use of personal technology: A phenomenological study. 2019.

[25] Andreas Gustav and Salah Kabanda. Byod adoption concerns in the south african financial institution sector. In *CONF-IRM*, page 59, 2016.

[26] Palesa Mphahlele. The impact of bring-your-own-device on work practices in the financial sector. Master's thesis, University of Cape Town, 2016.

[27] Aboeryzal Ahmed Koesyairy, Angga Kurniawan, Achmad Nizar Hidayanto, Nur Fitriah Ayuning Budi, and Rahmat M Samik-Ibrahim. Mapping internal control of data security issues of byod program in indonesian banking sector. In *2019 5th International Conference on Computing Engineering and Design (ICCED)*, pages 1–5. IEEE, 2019.

[28] Lizzy Oluwatoyin Ofusori. *Three-dimensional security framework for BYOD enabled banking institutions in Nigeria.* PhD thesis, 2019.

[29] Geoffrey K Sowek. *A framework for enhancing corporate data security in a bring your own device (Byod) environment: a case of government organizations in Kenya.* PhD thesis, Kca University, 2018.